港湾安全管理平台

用户手册

第一部分　安装港湾安全管理平台系统

第二部分　配置港湾安全管理平台系统

港湾网络

港湾安全管理平台用户手册

资料编号	P-1801****-20040520-110（手册编码尚未申请）
产品版本	V01R01B00
资料状态	发行

版权声明

© 港湾网络有限公司版权所有，并保留对本手册及本声明的最终解释权和修改权。

本手册的版权归港湾网络有限公司所有。未得到港湾网络有限公司的书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。港湾网络有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但港湾网络有限公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

Users' Manual Copyright and Disclaimer

Copyright

© Copyright Harbour Networks Limited. All rights reserved.

The copyright of this document is owned by Harbour Networks Limited. Without the prior written permission obtained from Harbour Networks Limited, this document shall not be reproduced and excerpted in any form or by any means, stored in a retrieval system, modified, distributed and translated into other languages, applied for a commercial purpose in whole or in part.

Disclaimer

This document and the information contained herein is provided on an "AS IS" basis. Harbour Networks Limited may make improvement or changes in this document, at any time and without notice and as it sees fit. The information in this document was prepared by Harbour Networks Limited with reasonable care and is believed to be accurate. However, Harbour Networks Limited shall not assume responsibility for losses or damages resulting from any omissions, inaccuracies, or errors contained herein.

手册使用说明

读者对象

本手册的读者对象为安装和使用港湾安全管理平台系统进行 SmartHammer 管理的系统管理员。本手册需要读者熟悉防火墙、以太网和组建局域网的概念和术语。

内容介绍

本手册详细介绍了港湾安全管理平台系统的安装和使用方法，使管理人员了解本系统并顺利完成系统安装与使用的指导文档。《港湾安全管理平台用户手册》共分为两个部分：

第一部分 安装港湾安全管理平台系统

通过阅读本部分内容，用户将对本系统的用途、特点和版本信息等有一个全面的了解，并可进行本系统的正确安装。具体包括以下内容：

章序号	题目	内容描述
第1章	港湾安全管理平台系统概述	简要讲述港湾安全管理平台系统的功能、特点及版本说明。
第2章	系统构建	讲述港湾安全管理平台系统的运行环境以及构建和安装、卸载方法。

第二部分 配置港湾安全管理平台系统

通过阅读本部分内容，用户将了解使用本系统的相关知识，并可利用本系统完成 SmartHammer 管理。具体包括以下内容：

章序号	题目	内容描述
第3章	相关知识	讲述与使用本系统相关的网络基本知识及其它相关知识。
第4章	系统启动	介绍系统后台服务和前台的组成、功能，以及如何启动它们，并进入管理系统。
第5章	用户管理	讲述用户管理的内容、作用和相关操作。
第6章	配置管理	讲述业务管理的内容、相关技术原理和操作。
第7章	日志管理	讲述日志管理的内容、作用和相关操作。

手册约定

手册中有关图标的约定如下：

图标	说明
注意	这个图标表示提醒用户注意事项。
提示	这个图标主要给出一些与正文相关的信息，同时给用户一些指引，协助用户更好的理解正文的内容。

获取技术支援

港湾网络有限公司建立了以总部技术支援中心、区域技术支援中心和本地技术支援中心为主体的完善的三级服务体系，并提供全天候 24 小时×365 天的电话热线服务。用户在产品使用及网络运行过程中遇到问题时请随时与港湾网络有限公司各地方的服务支持热线联系。请用户到www.harbournetworks.com获取各地服务支持热线电话。此外，用户还可通过港湾网络有限公司网站及时了解最新产品动态，以及下载需要的技术文档。

目录

第一部分 安装港湾安全管理平台系统

第 1 章 港湾安全管理平台概述 1-1

1.1 简介 1-1

1.1.1 系统组成 1-1

1.1.2 系统特点 1-2

1.2 版本说明 1-2

第 2 章 系统构建 2-1

2.1 硬件环境 2-1

2.2 软件环境 2-1

2.3 系统的安装 2-2

第二部分 配置港湾安全管理平台系统

第 3 章 相关知识 3-1

3.1 概述 3-1

3.2 基本知识 3-1

3.2.1 包过滤 3-1

3.2.2 安全域 3-2

3.2.3 IP Inspect（基于状态的资源控制） 3-2

3.2.4 NAT（网络地址转换） 3-3

3.2.5 NetFlow 3-4

3.3 操作系统 3-4

第 4 章 系统启动 4-1

4.1 概述 4-1

4.2 启动后台服务 4-1

4.3 启动前台程序 4-1

4.3.1 登录 4-2

4.3.2 前台主界面 4-2

第 5 章 用户管理 5-1

5.1 概述 5-1

5.2 网管软件用户管理 5-1

5.2.2 添加用户 5-2
5.2.3 删除用户 5-3
5.2.4 修改密码 5-3
5.3 主机用户管理 5-3
5.3.2 添加用户 5-4
5.3.3 删除用户 5-5
5.3.4 修改密码 5-5
第 6 章 配置管理 6-1
6.1 概述 6-1
6.2 系统配置 6-1
6.2.1 Vlan 管理 6-1
6.2.2 面板管理 6-4
6.2.3 系统管理 6-7
6.2.4 接口配置 6-8
6.2.5 透明网桥配置 6-10
6.3 安全特性 6-15
6.3.1 ACL 配置 6-15
6.3.2 IP Inspect 6-18
6.3.3 包过滤配置 6-19
6.4 网络特性 6-22
6.4.1 NAT 配置 6-22
6.5 路由功能 6-27
6.5.1 静态路由 6-27
第 7 章 日志管理 7-1
7.1 概述 7-1
7.2 Syslog 日志管理 7-1
7.3 NetFlow 日志管理 7-7

第一部分

安装港湾安全管理平台系统

1 港湾安全管理平台概述

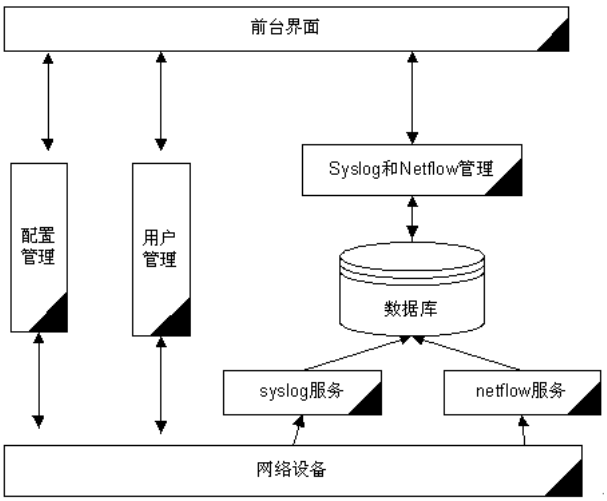
1.1 简介

港湾安全管理平台系统是港湾网络有限公司推出的 SmartHammer 管理软件。该管理软件主要用于 SmartHammer 的配置、日志和用户管理，可以为系统管理人员提供一个直观便捷、图形化的配置管理界面，从而取代通过命令行进行不同设备配置和管理的大量烦琐操作，减轻工作负担。

1.1.1 系统组成

港湾安全管理平台系统组成如下图所示：

图1-1 系统组成



各模块的主要功能如下：

- 前台界面：是图形化的 GUI 用户接口。通过前台界面，可以将用户关心的相关配置信息以直观的图形或表格形式呈现给用户，用户还可以更改这些信息。

- 配置管理：配置管理的主要功能包括：通过图形化界面配置防火墙的相关特性，用户可以及时地看到改变了配置的信息，便于用户操作。
- 用户管理：用户可以通过用户管理添加和删除用户，可以配置用户配置管理的级别等；通过用户管理，可以响应用户的申请，让用户通过用户管理系统帐号登录并使用本系统；通过权限配置给予不同操作员以不同权限来保证 SmartHammer 系统的分级管理，保证系统的安全性。
- 日志管理：日志管理是整个系统都必须使用的，能够记录 SmartHammer 运行的整个过程所产生的日志信息，保证对 SmartHammer 中的 Syslog 信息等操作做必需的记录。

1.1.2 系统特点

港湾安全管理平台系统的技术架构具有如下特点：

- c/s 设计：c/s 软件结构，使系统设置灵活；
- 多线程设计：支持多线程，提高系统性能，提高 CPU 利用率；
- 组件化设计：按照组件化的设计思想，后台服务全部是组件化实现；

1.2 版本说明

港湾安全管理平台系统 V1.00 for Windows 版本支持的设备种类包括：

- 港湾网络有限公司 SmartHammer G503/G503D 设备。
- 港湾网络有限公司的 SmartHammer M 系列设备

在本系统开始安装并运行以前，必须保证用户网络系统的连通性。

数据保存的基本方式包括：

- 数据库（Oracle、MySQL 或 PostgreSQL），主要用于保存用户信息、设备信息以及设备的故障及性能信息。

港湾安全管理平台系统默认使用的主要 Socket 端口包括：

- 端口 514（UDP）

- 端口 9898（UDP）
- 端口 80（TCP）

如果这几个端口被其它应用程序使用，港湾安全管理平台系统需另行配置才可正常运行。

2 系统构建

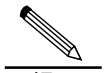
2.1 硬件环境

港湾安全管理平台系统安装在网管服务器上，其硬件配置要求如下：

- CPU 频率不小于 1.5GHz
- 硬盘容量不小于 40G 字节
- 内存不小于 512M 字节
- 具有网络连接设备

建议配置：

- HP PC Server ML-350 XEON 2.4G
- 40G SCSIHD
- 1024M 内存
- 100/1000M 以太网卡

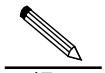


港湾安全管理平台系统的 V1.00 版本暂不支持 SUN 服务器。

2.2 软件环境

系统的软件环境主要包括：

- 操作系统：Windows 2000 Server / Professional，Windows XP
- 数据库：MySQL



本手册有关界面及操作的讲解全部基于 Windows 2000 Professional。

2.3 系统的安装

直接在安装程序下运行 setup.exe 即可。每一步都有相应的提示信息，用户可以使用默认选项，也可以改变默认选项。

注意

为了避免文件冲突，确保港湾安全管理平台系统正确安装和运行，请将港湾安全管理平台系统安装在一个独立目录下。

港湾安全管理平台系统安装完成后，可在 Windows 的“开始－>程序”中看到‘Harbour Security Manager’程序组，在程序组下可看到 ‘Configure Manager’和‘Log Manager’两个快捷方式，其中‘Configure Manager’用来启动港湾安全管理平台系统的配置界面前台，‘Log Manager’用来启动港湾安全管理平台系统的日志界面前台。

提示

卸载说明:

用户在“控制面板—>添加/删除程序”中卸掉本系统。在卸载本系统之前，请先在控制面板—管理工具—服务中禁止 Syslog Deamon 和 Netflow Deamon 两个服务，否则会导致卸载失败

第二部分

配置港湾安全管理平台系统

3 相关知识

3.1 概述

本章对包过滤、安全域、IP inspect（基于状态的资源控制）、NAT 和 NetFlow 技术等进行了简要介绍。了解和掌握这些知识，将有助于您更好的理解和使用港湾安全管理平台系统。

3.2 基本知识

3.2.1 包过滤

包过滤（Packet Filter）是在网络层中对数据包实施有选择的通过，依据系统事先设定好的过滤逻辑，检查数据流中的每个数据包，根据数据包的源地址或者目标地址，以及包所使用端口确定是否允许该类数据包通过。

1. 简单的包过滤

简单的包过滤，防火墙所看到的网络数据包是孤立存在的，允许和拒绝完全取决于包自身包含的信息（源地址、目的地址、端口号等），是无状态的，防火墙对每个数据包都进行独立的规则检测，效率非常低，而且功能非常有限，无法真正实现对被保护区域的保护功能。

2. 基于状态的包过滤

基于状态的包过滤，提供了更高的效率和安全性，通过跟踪网络包的状态来决定对网络包的处理（放行还是过滤），不仅考虑每个网络包，而且考虑网络包的历史关联性。在进行规则匹配时，将包的连接状态记录下来，同一连接的包，只检查第一个包，以后该连接的包就可以不用通过规则检查，而只需要检查状态表里该包所属的连接状态，如果该连接的包状态中显示已通过检查，表示该网络包属于已建立的

合法连接，则不需要对该包进行检查，可以通过，同时更新状态表。

这样就极大的提高了包过滤的效率。

3.2.2 安全域

设备的每个接口(物理接口或虚拟接口)所连接的网络可以属于一个不同的安全域，设备本身也作为一个安全域。

设备具有 6 个内置安全域：

自由域（unrestricted)、普通域（general)、限制域（restricted)、控制域（controlled)、保护域（protected)、隔离域（isolated）

用户还可以根据自己的需求自定义安全域，这些自定义的安全域是基于限制域、控制域或保护域的子域。

不同的安全域之间的访问，受到其安全策略、安全级别、访问控制策略（ACL）的控制。

表3-1 安全域基本访问策略

离开 / 进入	自由域	普通域	限制域	控制域	保护域	隔离域
自由域	√	×	×	×	×	×
普通级	√	√	×	×	×	×
限制域	√	√	★	×	×	×
控制域	√	√	√	★	×	×
保护域	√	√	√	√	★	×
隔离域	×	×	×	×	×	×

√表示可访问，×表示不可访问，★表示根据安全级别和访问控制策略（ACL）确定

3.2.3 IP Inspect（基于状态的资源控制）

一般的网络设备（包括防火墙产品)、计算机在受到大量 DOS（Denial of Service）攻击时，会因为所有的连接资源都被攻击所占用，使得正常数据包无法通过设备，从而阻碍正常的通信。

IP Inspect 通过监视所有连接的状态，限制特定协议的连接数目和高低警戒线，能够在以下几种情况下，有效的防止设备浪费连接资源，保证正常数据通过：

- 连接长时间没有应答，一直处于半连接状态；
- 连接已经建立，但长时间没有数据穿过；
- 设备受到半连接攻击；
- 某种协议的网络病毒存在；

IP Inspect 还可以通过限制发起连接的外部主机的连接数，以及被访问的内部主机或内部主机某个端口的连接数，保护设备内部某些主机，使其不受攻击。

3.2.4 NAT（网络地址转换）

NAT 是指在一个网络内部，根据需要可以随意自定义的 IP 地址，而不需要经过申请。在网络内部，各计算机间通过内部的 IP 地址进行通讯。而当内部的计算机要与外部 internet 网络进行通讯时，具有 NAT 功能的设备负责将其内部的 IP 地址转换为合法的 IP 地址（即经过申请的 IP 地址）进行通信。

1. 基于源地址的 NAT

基于源地址的 NAT 可以用于在内部网络用户访问公有网络地址时将内部网络用户使用的内部 IP 地址转换为公有网络地址。这样的实现不仅可以解决企业公有网络地址不足的问题，同时对公有网络来说，访问全部是来自于经过防火墙转换后的地址，并不认为是来自内部网络的某个地址，可以有效的隐藏内部网络结构，减少对内部的攻击。

动态 NAT（Dynamic NAT）：

指动态的将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP 地址，不同的连接可能映射到地址池中不同的地址；

PAT：

指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分。

静态 NAT：

这是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当

于在内、外网之间建立了一条双向通道。

2. 基于目标地址的 NAT

基于目标地址的 NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与静态 NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。

3.2.5 NetFlow

NetFlow 技术能够有效地提供网络流量测量，包括流量计帐和分析，基于应用的计帐和分析，也可以根据网络流量分布来查看网络带宽，是否足够以便升级网络，或者监视网络分析是否受到 DOS 攻击。

NetFlow 能够提供非常有价值的信息：当前什么用户在使用网络，什么应用，什么时间段利用，以及网络流量的流向。NetFlow 可以把设备通过的流量以 UDP 包形式发送给收集器，由收集器收集并分析、整理，提供给网络管理员整个网络利用情况，可以做到实时收集实时分析，随时掌握整个网络。

3.3 操作系统

UniWorks VPN Manager 系统 V1.00 for Windows 版本的操作系统为 Windows 2000 Server / Professional 或 Windows XP。

本手册主要涉及 Windows 2000 操作系统的功能或操作，但不作详细说明。有关 Windows 2000 操作系统的知识，请用户参考操作系统随带的文档资料。

4 系统启动

4.1 概述

用户要利用港湾安全管理平台系统进行 SmartHammer 防火墙的管理，首先需要确定港湾安全管理平台系统的后台服务正在运行。确定后台服务正在运行后，用户便可启动港湾安全管理平台系统的前台程序。

4.2 启动后台服务

港湾安全管理平台系统的后台服务包括：

- mysql 服务：主要负责数据库的连接、数据的实时存储和历史查询。
- syslog 服务：负责收集和解析 syslog 日志和数据库的连接。
- netflow 服务：负责收集和解析 netflow 日志和数据库的连接。

一般情况下，这三个服务会在每次启动 Windows 系统时自动启动，不需要用户手工干涉。如果用户想查看三个服务的状态，只需启动控制面板－〉管理工具－〉服务。Mysql 服务的名称为 MySql；syslog 服务的名称为 Syslog Deamon；netflow 服务的名称为 NetFlow Deamon。用户可以在服务中查看三个服务的状态，并可以手工的对其进行操作。

4.3 启动前台程序

港湾安全管理平台系统的前台程序主要用于系统配置管理、用户管理以及日志管理。

港湾安全管理平台系统前台程序提供了友好的图形用户界面，可以方便用户简单快捷地管理配置 SmartHammer 防火墙，方便快捷地查询系统日志历史记录，并根据历史数据有效的生成报表，方便用户的管理和维护，提高工作效率。

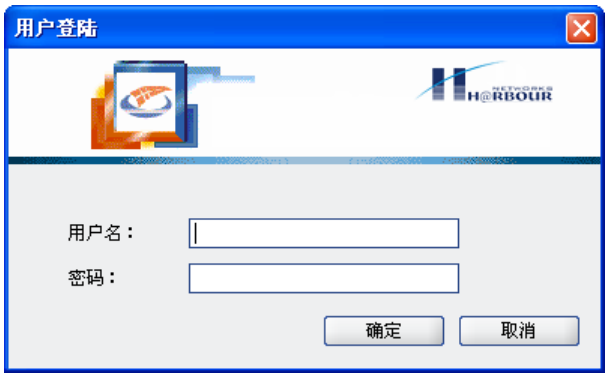
港湾安全管理平台系统前台程序可以在后台服务正确启动以后随时启动。启动方法

为：打开 Windows 的“开始—>程序－>Harbour Security Manager－>Configure Manager”，启动港湾安全管理平台系统前台。

4.3.1 登录

前台程序启动以后用户看到第一个界面就是系统的登录界面，用户需要先进行系统用户验证：

图4-1 用户登录



用户第一次登录时使用系统预置的用户名和密码：

- 用户：admin
- 密码：harbour

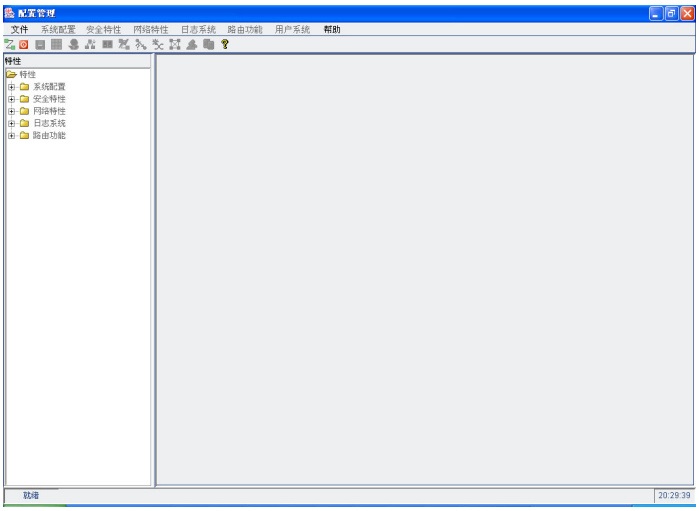
为了保证系统的安全性，建议用户登录系统后首先修改默认密码。具体方法请参见第 5 章 用户管理的相关内容。

4.3.2 前台主界面

港湾安全管理平台系统登录后的主界面如下图所示：

登录后的主界面如下图所示：

图4-2 登录后主界面



用户登录后，如果想对 SmartHammer 进行配置，还必须进行连接。方法是点击文件菜单下的“连接”子菜单，如图4-3所示：用户需要输入想要连接的 SmartHammer 防火墙的 IP 地址、用户名和密码。输入正确后，按连接键进行连接。连接成功后，主界面如图4-4所示。这时，用户就可以对其进行配置管理了。

图4-3 连接界面

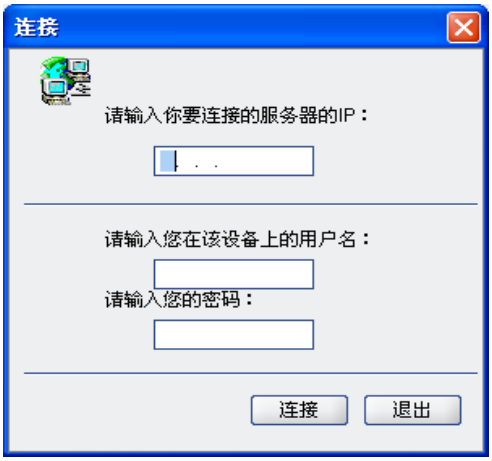
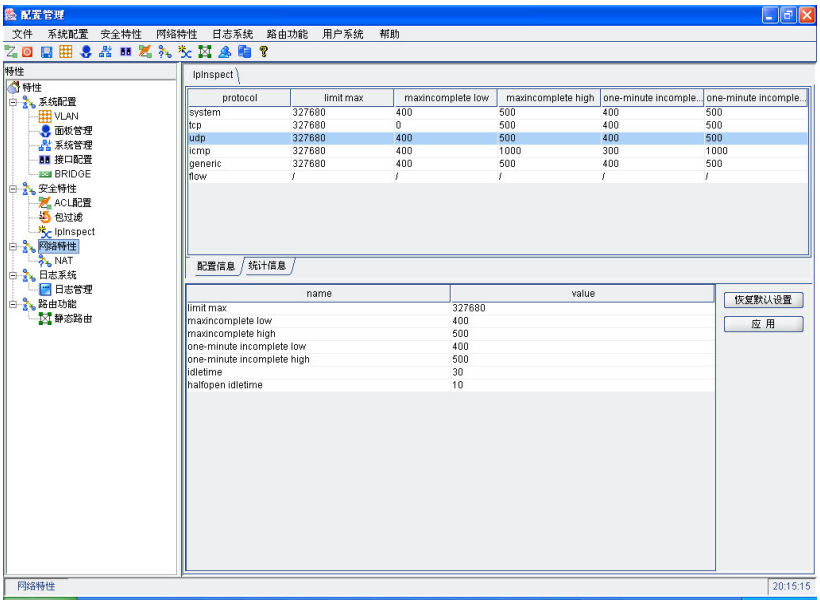


图4-4 连接成功后的主界面



5 用户管理

5.1 概述

用户管理主要包括网管软件用户管理和主机侧用户管理。

通过用户管理，用户可以方便地添加和修改用户基本资料。

Harbour Secutiry Manager 系统安装完成后，系统会创建一个默认用户：

- 用户：admin
- 密码：harbour

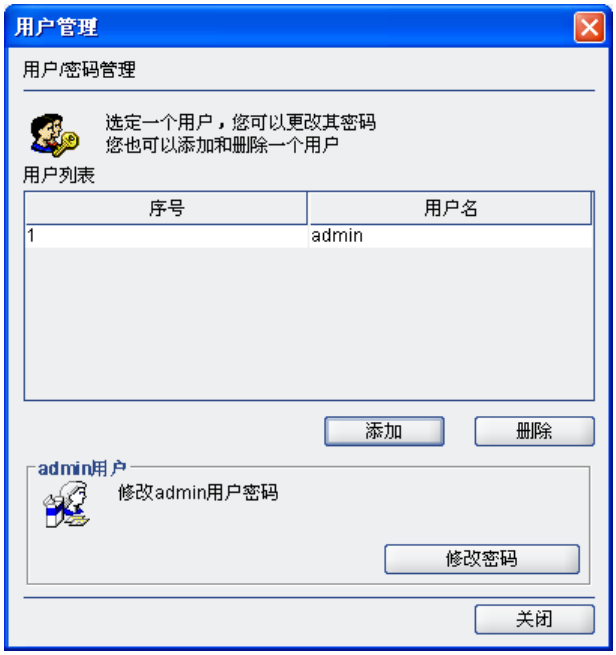
使用这个默认用户可以登录本系统软件，进行配置管理。

5.2 网管软件用户管理

用户管理中主要包括添加用户、修改用户密码以及删除用户。

用户在配置管理界面下点击用户系统菜单下的子菜单“系统用户管理”进入网管软件系统用户管理，如图图 5-1 所示。

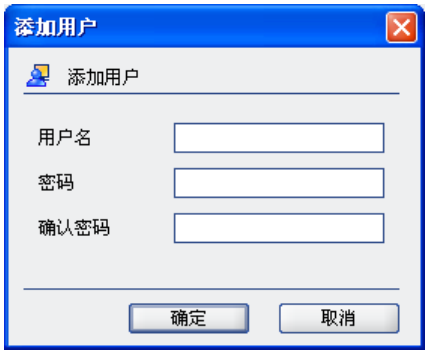
图5-1 系统用户管理



5.2.2 添加用户

如图 5-2 所示，用户需要输入用户名和密码，确认密码。要注意的是，密码不能少于 6 位。按“确定”键添加成功。

图5-2 添加用户



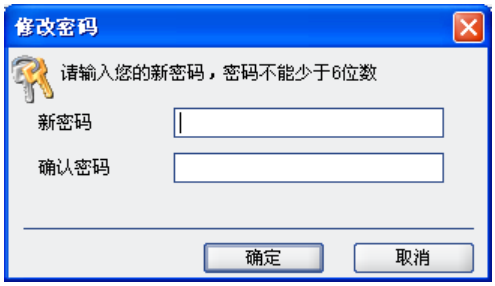
5.2.3 删除用户

用户在用户管理主界面下选中一个用户，按删除键进行删除。

5.2.4 修改密码

用户在用户管理主界面下选中一个用户，按“修改密码”键进行进行密码的修改。如图 5-3 所示，用户需要输入新密码和确认密码，密码不能少于 6 位数。按“确定”键修改成功。

图5-3 修改密码



5.3 主机用户管理

主机用户管理中主要包括添加用户、修改用户密码以及删除用户。

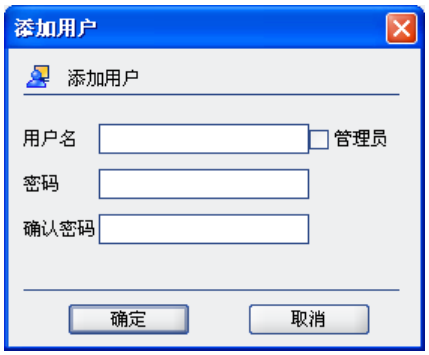
主机用户在配置管理界面下点击用户系统菜单下的子菜单“主机用户管理”进入网管软件系统用户管理，如图 5-4 所示。

图5-4 主机用户管理

5.3.2 添加用户

如图 5-5 所示，用户需要输入用户名和密码，确认密码。如果添加的是管理员用户，请选中管理员复选框；要注意的是：密码不能少于 6 位。按“确定”键添加成功。

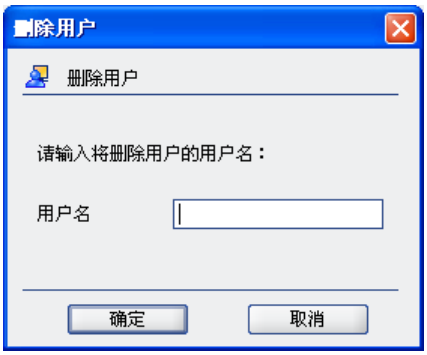
图5-5 添加用户



5.3.3 删除用户

如图 5-6 所示，输入您要删除的用户名，按“确定”键进行删除。

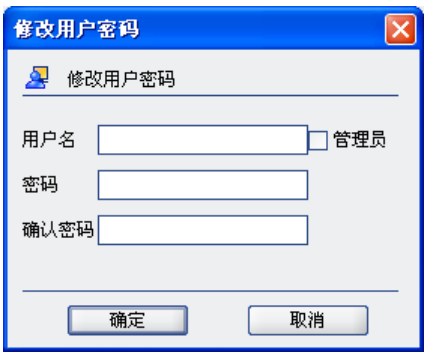
图5-6 删除用户



5.3.4 修改密码

如图 5-7 所示，输入您要修改用户的用户名，新密码及确认密码。需要注意的是：如果该用户是管理员用户，请选中“管理员”复选框。按“确定”键进行修改。

图5-7 修改用户



6 配置管理

6.1 概述

配置管理是整个港湾安全管理平台系统的核心部分。

港湾安全管理平台系统的配置管理主要是对 SmartHammer 配置命令的管理，主要功能包括系统配置、安全特性、网络特性和路由功能。

6.2 系统配置

系统配置部分包括 Vlan 管理、面板管理、系统管理、端口配置、桥管理五个部分。下面分别讲述以下各部分的使用方法。

6.2.1 Vlan管理

在一个物理局域网内，通过对交换机端口的划分，将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发；通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。对于以端口划分的 VLAN 而言，任何一个端口的集合（甚至设备上的所有端口）都可以被看作是一个 VLAN。VLAN 的划分不受硬件设备物理连接的限制，用户可以通过命令灵活地划分端口，创建定义 VLAN。使用 VLAN 的优点如下：

VLAN 能帮助控制流量

在传统网络中，不管是否必要，大量广播数据被直接送往所有网络设备，从而导致网络堵塞。而 VLAN 的设置能够使每个 VLAN 只包含那些必须相互通信的设备，从而减少广播、提高网络效率。

VLAN 提供更高的安全性

每个 VLAN 中的设备只能与本 VLAN 中的设备通信。例如，如果 VLAN Market 的设备要和 VLAN Sales 的设备通信，则只有通过路由器才能进行，在没有三层路由设备的情况下两个部门不能直接通信，从而提高了网络安全性能。

VLAN 使网络设备的变更和移动更加方便

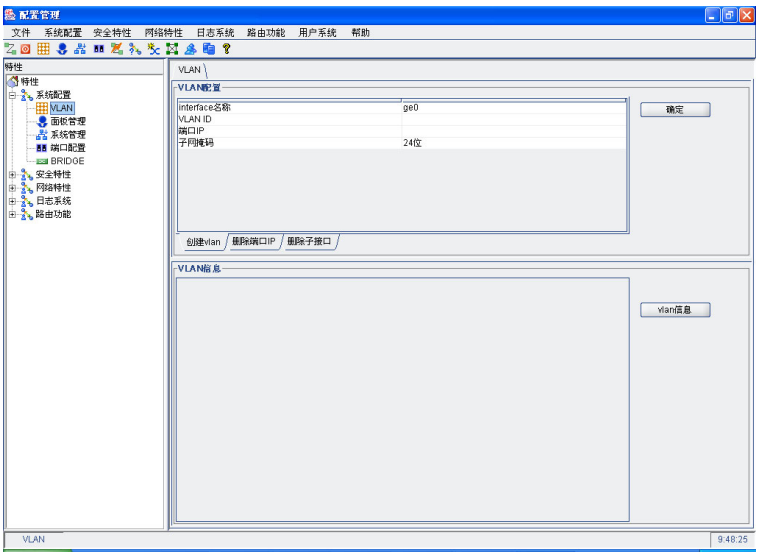
在传统网络中，网络管理员不得不在网络设备的变更和移动上花费大量的时间和精力。如果用户移动到另一个不同的子网，那么每个终端的地址都得重新设置。而使用 VLAN 则不需要这些复杂繁琐的设置。

SmartHammer 防火墙起到连接不同的 VLAN 的作用，它各有一个端口连接到这些 VLAN 上，从 SmartHammer 防火墙的角度与从终端的角度来看，整个网络看起来像自然的局域网一样连接。

SmartHammer 防火墙只实现对 VLAN 的终结功能。

Vlan 的管理界面如图 6-1 所示。分为创建 Vlan、删除端口 IP、删除子接口三项。

图6-1 Vlan 管理



1．创建 Vlan

如图 6-1 。用户在 interface 名称一栏选定所要创建 vlan 的接口，选定好接口后，在 VLAN ID 一栏输入 vlan ID 的值，这个值必须为整数。如果用户想在新创建的

vlan 接口上添加 IP 地址，那么可以在端口 IP 一栏输入 IP 地址，并选定子网掩码位数，按右侧的确定键即可配置成功。如果用户暂时不想配置端口的 IP 地址，则可以不用输入端口 IP 和选定掩码位数，直接按确定键即可创建成功。

2．删除端口 IP

如图 6-2 。用户选择删除端口 IP 属性页，在第一栏选择要删除的端口 IP 的接口名称，按“确定”键即可配置成功。

3．删除子接口

如图 6-3 。用户选择删除子接口属性页，在第一栏选择要删除的子接口，按确定键即可配置成功。

用户还可以按下面的 Vlan 信息键查看所有创建的 Vlan 信息。

图6-2 删除端口 IP

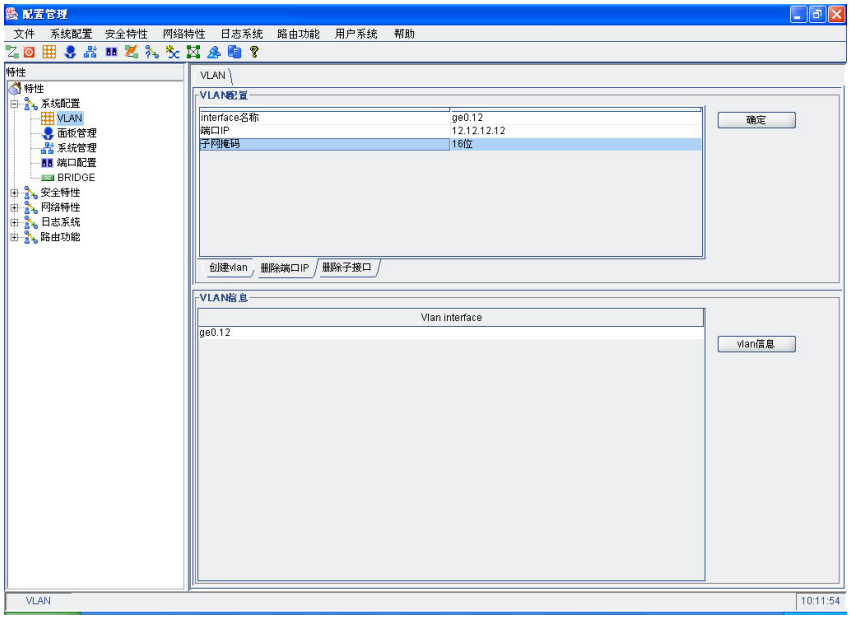
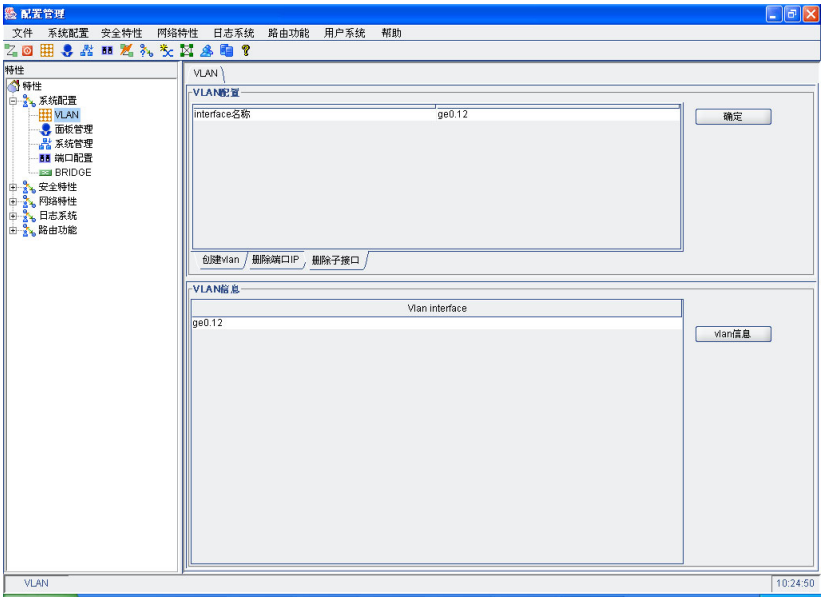


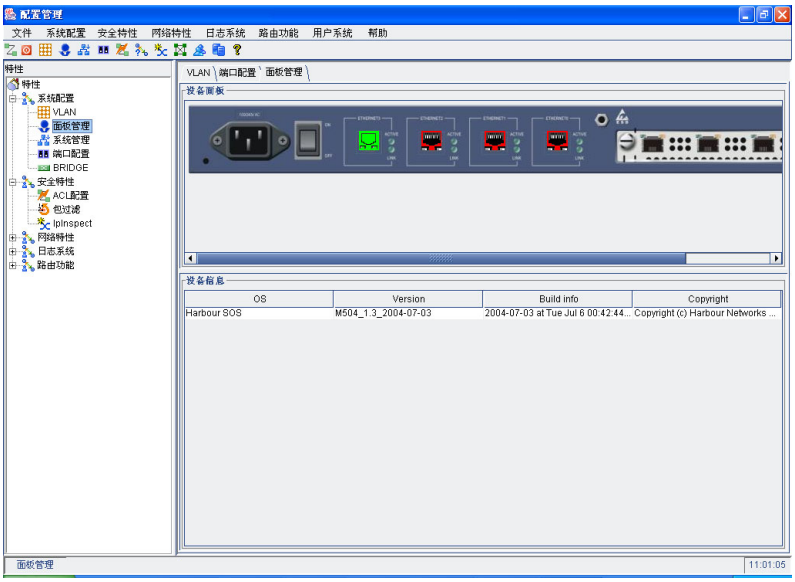
图6-3 删除子接口



6.2.2 面板管理

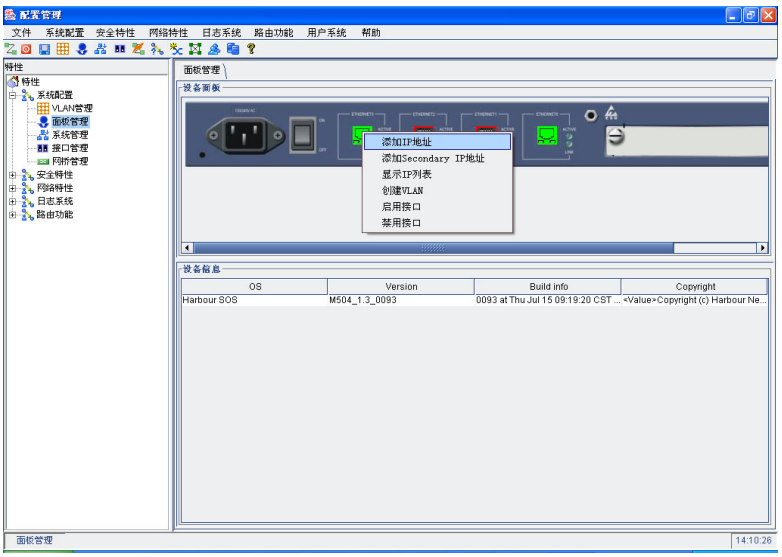
面板管理提供给用户形象直观的设备面板视图，供用户对接口进行操作，并可以随时监控接口的状态。面板管理如图 6-4 所示。

图6-4 面板管理



用户可以观看设备的信息，可以在连通的接口上进行添加 IP 地址、添加 Secondary IP 地址、显示 IP 列表、创建 Vlan 等一系列的操作，如图 6-5 所示。

图6-5 面板管理操作



添加 IP 地址如图 6-6 所示，用户输入 IP 地址和子网掩码按确定即可。

图6-6 添加 IP

添加 Secondary IP 地址如图 6-7 所示。用户输入 IP 地址和子网掩码按确定即可。

图6-7 添加 Secondary IP

显示 IP 列表如图 6-8 所示，会把该接口的所有 IP 地址列出来，用户还可以选定一行进行删除。

图6-8 显示 IP 列表

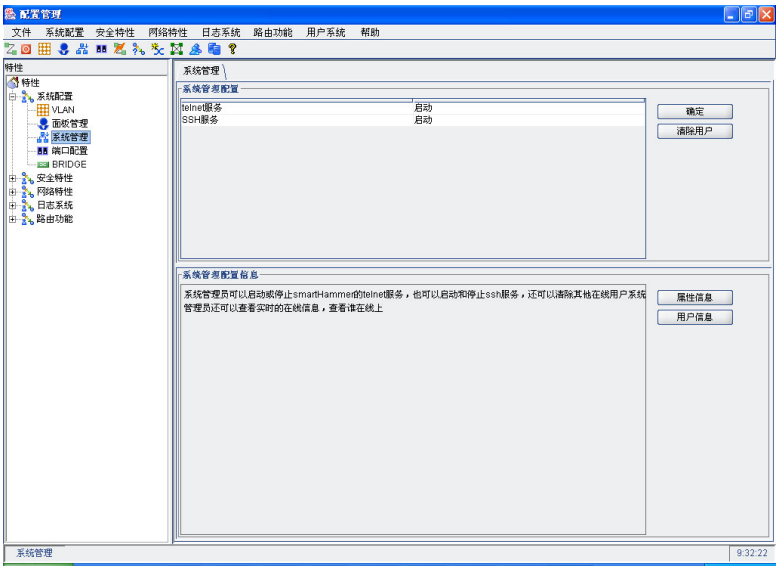
创建 Vlan 如图 6-9 所示，用户输入 Vlan ID 和 IP 地址和子网掩码，按“确定”键即可创建成功。

图6-9 创建 VLAN

6.2.3 系统管理

系统管理中，用户可以查看当前 SmartHammer 中 Telnet 服务和 SSH 服务的状态，用户还可以改变当前服务的状态，方法是选择启动或停止，按确定键使其生效。用户还可以清除其他用户，如果有其他用户通过 Telnet 登陆 SmartHammer，那么通过清除其他用户功能，可以使其他用户强制下线。用户还可以通过点击用户信息按钮查看实时的用户在线信息，看有哪些用户在线上。属性信息功能提供给了用户的简单的帮助信息。系统管理界面如下图 6-10 所示：

图6-10 系统管理

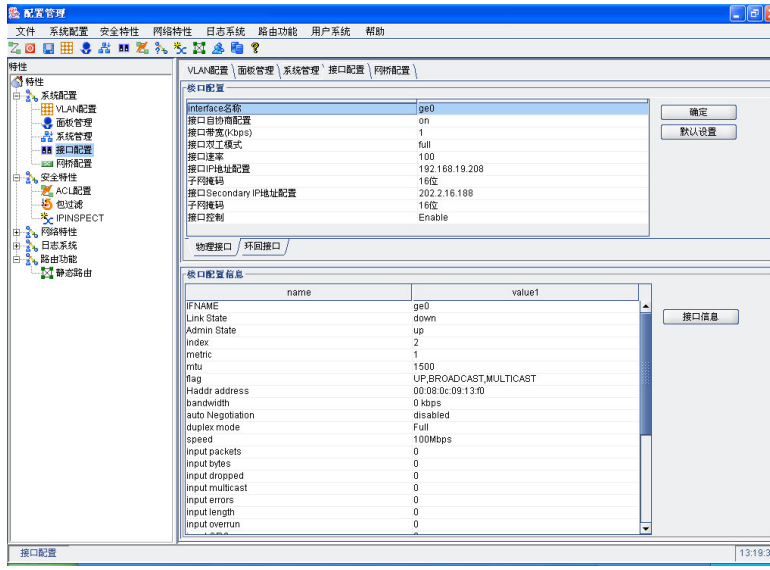


6.2.4 接口配置

接口配置分为物理接口配置和环回接口配置两种。

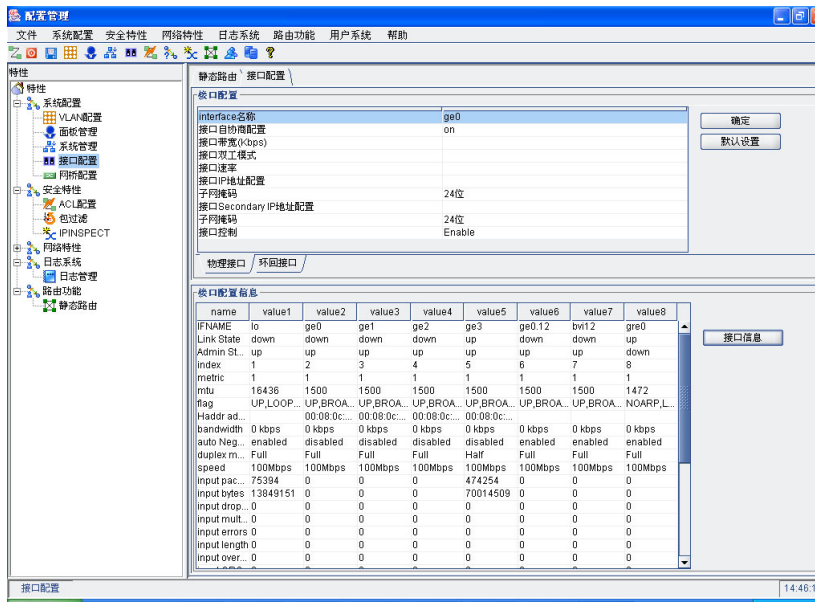
1．物理接口配置如图 6-11 所示：

图6-11 物理接口配置



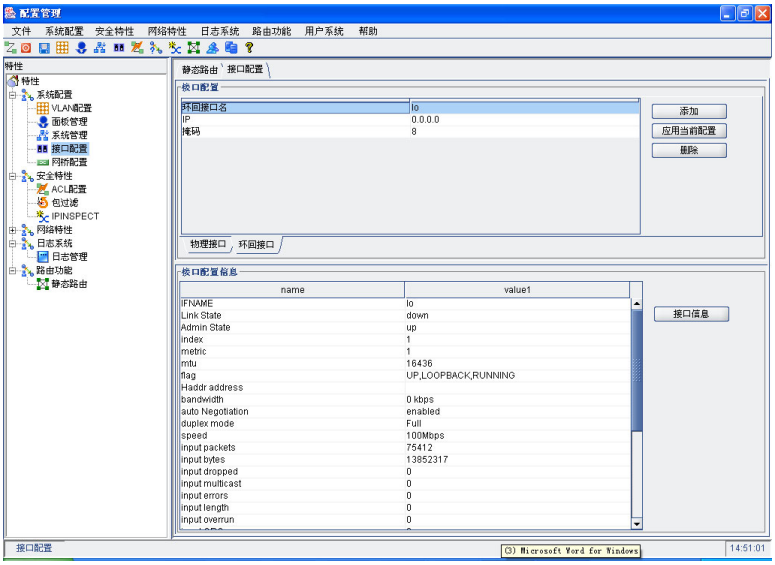
用户可以查看某个物理接口的信息，也可以用鼠标双击来改变功能选项配置。按“确定”键后使其生效。按默认设置使选定的接口恢复默认数值，按下面的接口信息可以查看所有的接口信息，如图 6-12 所示。

图6-12 显示接口信息



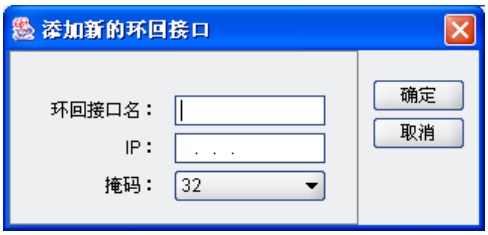
2．环回接口配置如图 6-13 所示：

图6-13 环回接口配置



用户可以选择已有的环回接口，然后配置好其 IP 地址，子网掩码，按应用当前配置键使其生效；用户还可以按添加键添加环回接口，弹出的窗口如图 6-14 所示，用户输入环回接口的名称和 IP 地址后，选择子网掩码的位数后按确定键即可添加成功。用户选定某个环回接口，按删除键即可将该环回接口删掉。

图6-14 添加环回接口



6.2.5 透明网桥配置

1. 概述

透明网桥功能：最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化。透明

网桥具有以下特征：

- 杂侦听和存储转发能力
- 点学习能力
- 生成树算法

透明网桥使用最方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，也不要设置地址开关和加载路径选择表参数，对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。透明网桥接收来自各局域网发送的帧，并将它送到目的局域网。它的缺点是不能最优地利用系统的带宽，只能用于分支拓扑结构的互连网络中。

2．配置

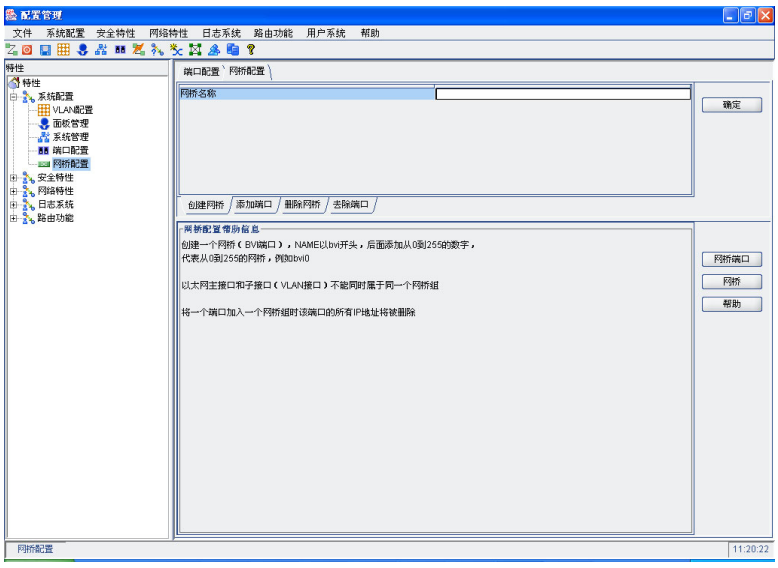
在 SmartHammer 设备上是通过配置 BVI（Bridge-group Virtual Interface）接口实现透明网桥功能。

一个 BVI 接口代表一个网桥，将不同的端口（物理或虚拟端口）加入同一个网桥中，从而可以实现在不同端口之间的桥接交换，配置为同一个网桥组中的所有端口属于同一个二层的广播域。

SmartHammer 可以实现在混合模式下工作，即在不同的 BVI 之间或 BVI 与其它的端口之间可以实现路由的能力。

1）创建网桥，如图 6-15 所示：

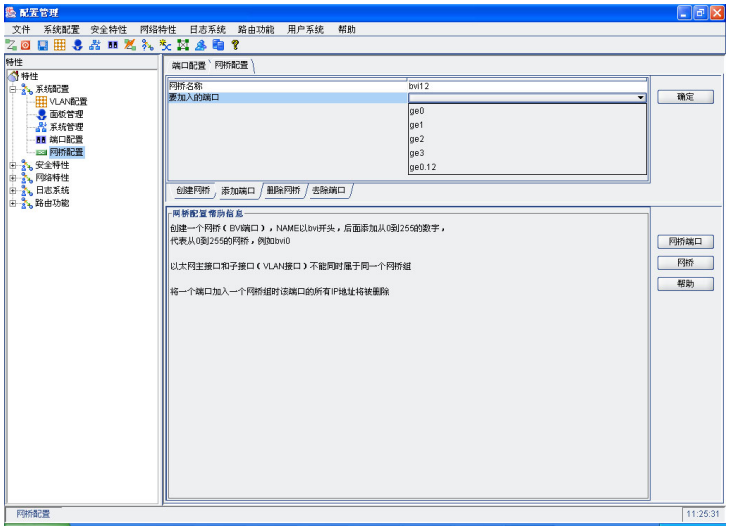
图6-15 创建网桥



在网桥名称对应的输入框内输入要创建的网桥名称，按确定键使其生效。要注意的是，网桥名称一定要以 bvi 开头，后跟数字，范围为 0-255 之间，例如 bvi0。

1） 添加端口，如图 6-16 所示：

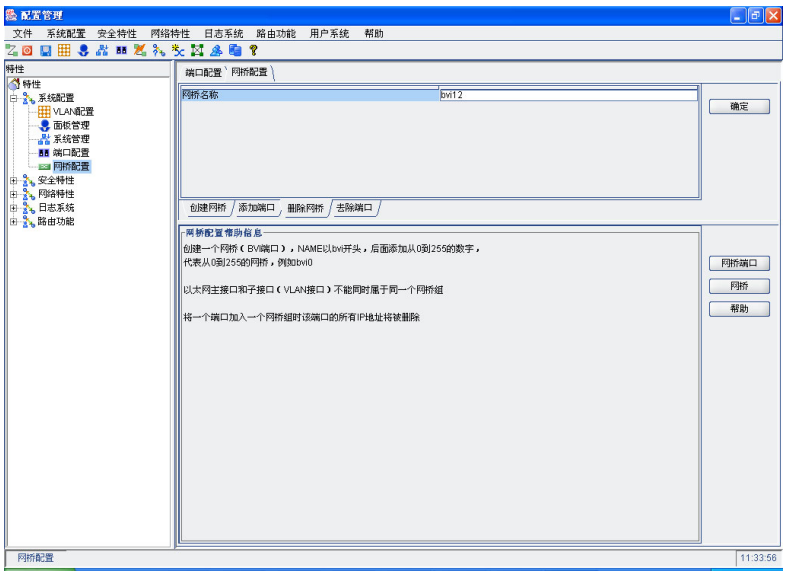
图6-16 添加端口



用户首先要选定好已存在的网桥组，示例为 bvi12，然后选择要加入该网桥组的端口，选定好后按确定键使其生效。

2） 删除网桥，如图 6-17 所示：

图6-17 删除网桥

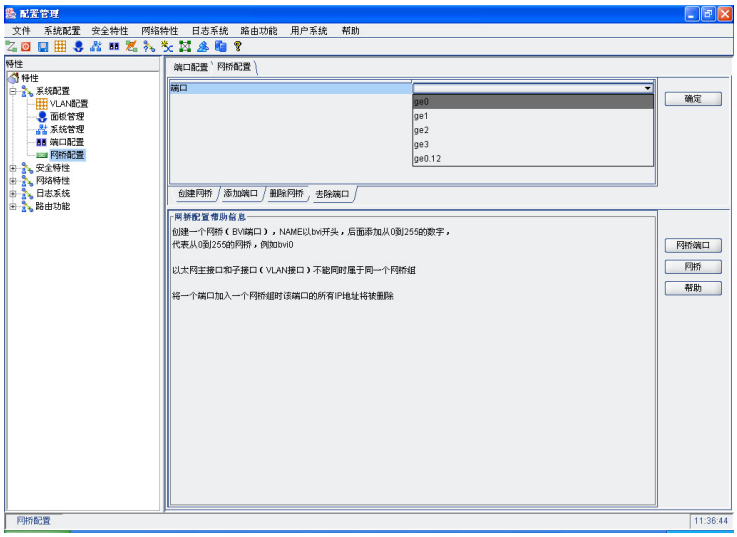


用户在网桥名称所对应的一栏中选定所要删除的网桥名称，然后按确定键使其生效。

3） 去除端口，如图 6-18 所示：

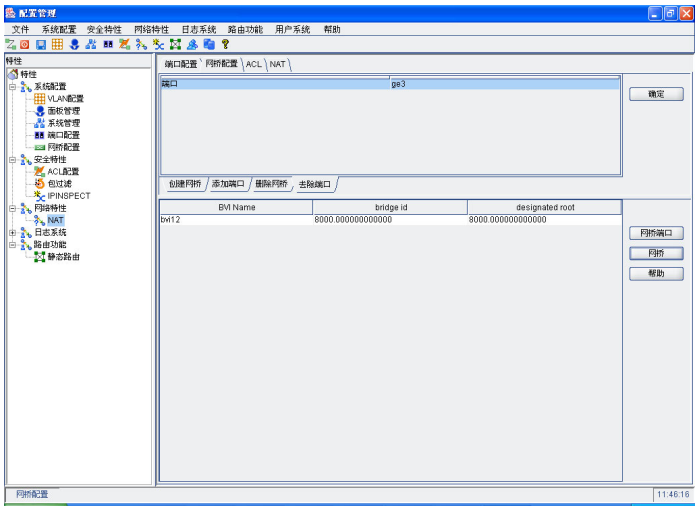
用户选择好要从网桥组中去除的端口，然后按确定键使其生效。

图6-18 去除端口



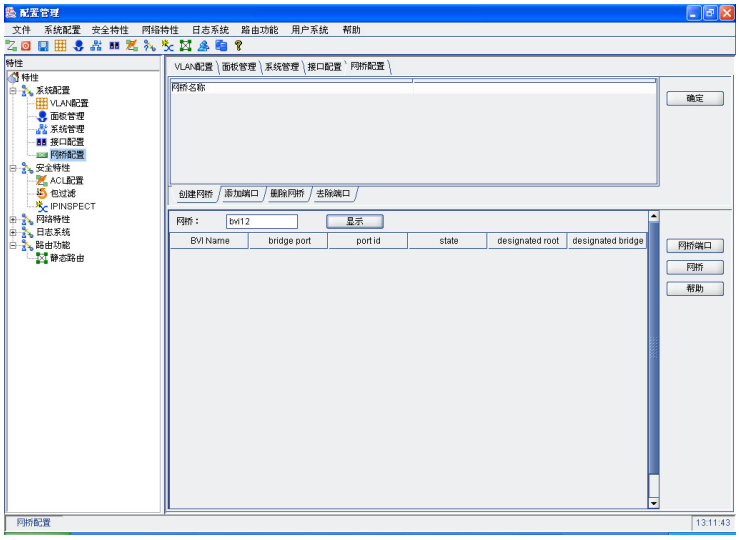
用户还可以通过点击网桥键来查看当前的网桥信息，如图 6-19 所示：

图6-19 查看网桥信息



用户还可以通过点击网桥端口按钮来查看某个网桥组的详细信息。如图 6-20 所示：在编辑框中输入网桥的名称，按显示按钮就会列出相关的信息。

图6-20 查看网桥的详细信息



6.3 安全特性

6.3.1 ACL配置

ACL 及 Access-list，主要为访问控制提供包过滤条件，另外也为带宽管理、入侵检测、应用代理等提供过滤规则，找出满足条件的数据包。ACL 本身并不直接起作用，必须与其它指令结合使用。

1．ACL 概述

ACL 相当于过滤规则，找出满足条件的数据包，ACL 根据 listid 主要分为以下几类：

<1-99>：标准 ACL，只能使用源 IP 进行过滤；

<100-199>：扩展 ACL，提供基于源 IP 和目标 IP 的过滤；

<200-299>：链路层 ACL，提供基于链路层协议和 MAC 地址的过滤；

<700-799>：链路层 ACL，提供基于 MAC 地址的过滤；

<1300-1999>：标准 ACL，提供基于源 IP 以及源端口的过滤；

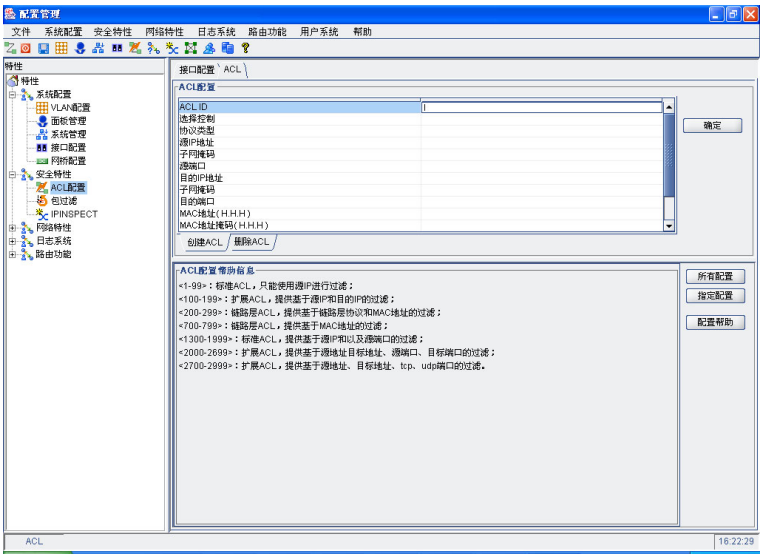
<2000-2699>：扩展 ACL，提供基于源地址、目标地址、源端口和目标端口的过滤；

<2700-2999>：扩展 ACL，提供基于源地址、目标地址、tcp、udp 端口的过滤。

2．ACL 配置

创建 ACL 如图 6-21 所示。

图6-21 创建 ACL

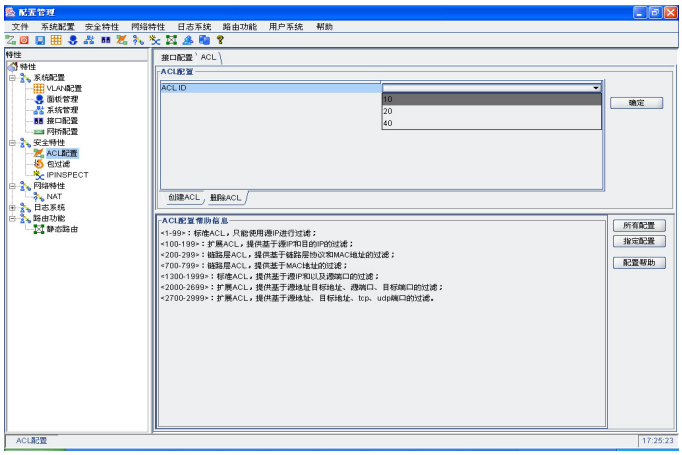


用户首先要输入 ACL ID 的值，该值是一个 1-2999 之间的一个整数，然后用户选择选择控制项进行选择允许访问还是拒绝访问。如果用户输入的 ACL ID 数值是在 1-99 之间，那么协议类型、源端口、目的 IP 地址、子网掩码、目的端口、MAC 地址、MAC 地址掩码、MAC 协议、MAC 协议掩码都为不可编辑状态；如果用户输入的 ACL ID 数值是在 100-199 之间，那么源端口、目的端口、MAC 地址、MAC 地址掩码、MAC 协议、MAC 协议掩码都为不可编辑状态；如果用户输入的 ACL ID 数值是在 200-299 之间，那么协议类型、源 IP 地址、子网掩码、源端口、目的 IP 地址、子网掩码、目的端口都为不可编辑状态；如果用户输入的 ACL ID 数值是在 700-799 之间，那么目的 IP 地址、子网掩码、目的端口、MAC 地址、MAC 地址掩码、MAC 协议、MAC 协议掩码都为不可编辑状态；

如果用户输入的 ACL ID 数值是在 2000-2699 之间，那么 MAC 地址、MAC 地址掩码、MAC 协议、MAC 协议掩码都为不可编辑状态；如果用户输入的 ACL ID 数值是在 2700-2999 之间，那么 MAC 地址、MAC 地址掩码、MAC 协议、MAC 协议掩码都为不可编辑状态。

删除 ACL 如图 6-22 所示。

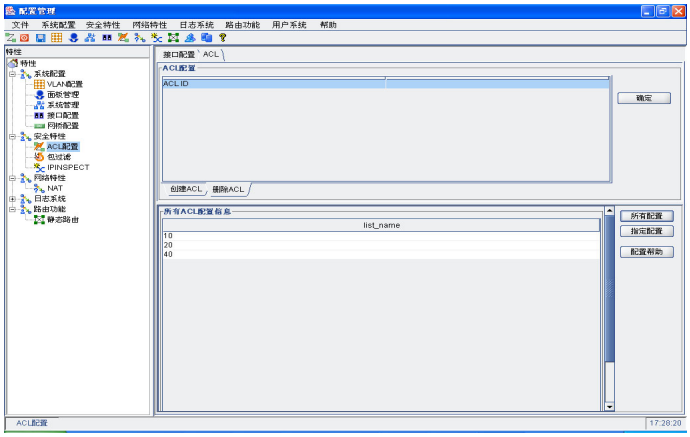
图6-22 删除 ACL



用户选定要删除的 ACL，按确定后即可删除成功。

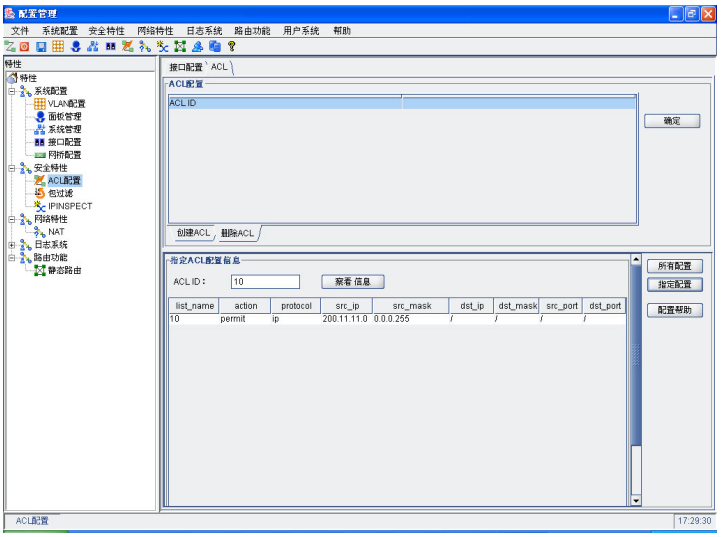
用户还可以通过点击所有配置按钮来查看所有的 ACL 配置信息。如图 6-23 所示。

图6-23 显示所有配置



用户也可以通过点击指定配置按钮，然后在显示的界面中输入已有的 ACL ID 的值来查看其详细信息。如图 6-24 所示。

图6-24 显示指定配置信息



6.3.2 IP Inspect

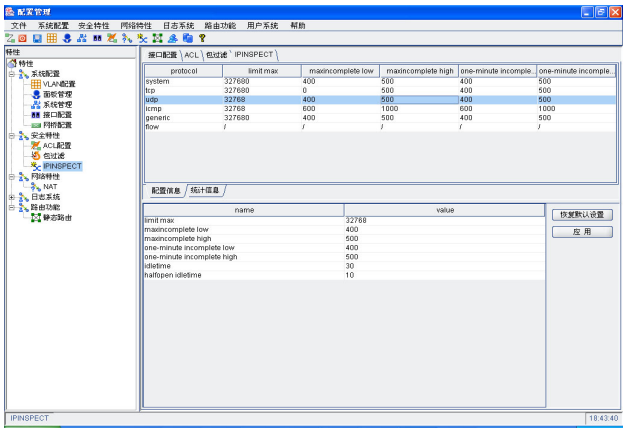
IP Inspect 可以有效的保证当设备受到大量 DOS（Denial of Service）攻击时，不会因为所有的连接资源都被攻击所占用而妨碍正常数据通过，还可以保护设备内部某些主机不受 DOS 攻击。

IP Inspect 分为配置信息和统计信息两种。

1．配置信息

如图 6-25 所示，点击配置信息中的某一行，在下面会显示其详细信息；用户还可以对详细信息进行修改，方法是用鼠标双击下面详细信息的值，修改后按应用键修改成功。用户按恢复默认设置可以是修改过的值恢复为默认的值。

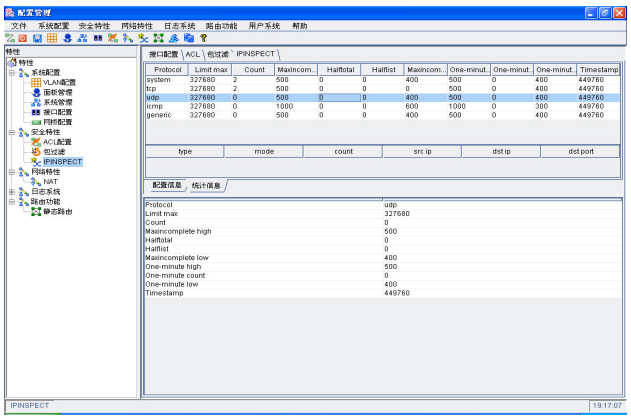
图6-25 配置信息



2．统计信息

如图 6-26 所示，点击统计信息中的某一行，在下面会显示其详细信息；这里要注意的是，统计信息不可更改。

图6-26 统计信息



6.3.3 包过滤配置

1．本地设置

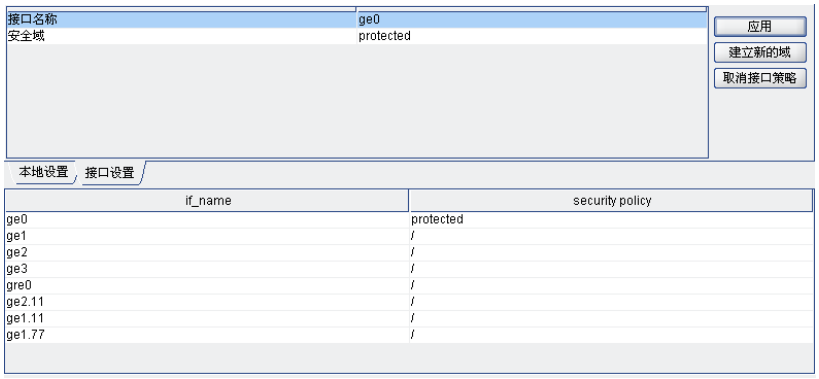
如图 6-27 所示，用户需要选择安全域，按应用键即可配置成功，所选的安全域会同时出现在安全策略列表中。按取消本地策略键即可取消配置。

图6-27 本地设置

2．接口设置

如图 6-28 所示，用户需要选择接口名称和安全域，按应用键即可配置成功，配置信息会同时显示在列表中。按取消本地策略键即可取消本地配置。

图6-28 接口设置



3．自定义安全域

用户单击图 6-27 或图 6-28 中的“建立新的域”按钮，即可自定义安全域，如图 6-29 所示。

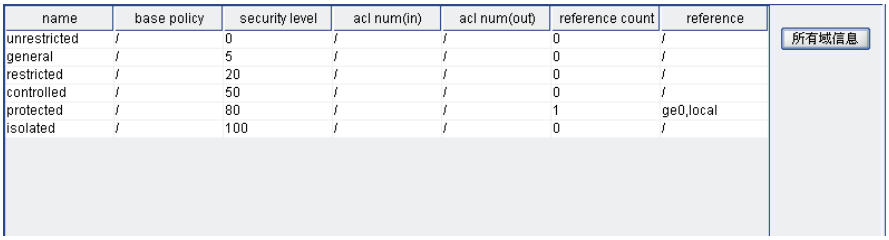
图6-29 自定义安全域

添加安全域需要用户输入新的域名、等级，选择继承域、in ACL 和 out ACL，按确定键即可添加成功。删除安全域需要用户选择安全域，按删除键即可删除。

4．显示域信息

如图 6-30 所示，用户按所有域信息键即可显示所有域的信息。

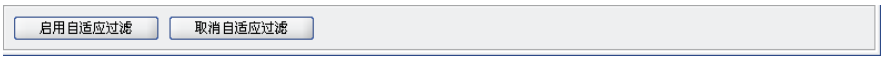
图6-30 显示域信息



5．启用（取消）自适应过滤

如图 6-31 所示，用户按启用自适应过滤键即可启用自适应过滤功能，用户按取消自适应过滤键即可取消自适应过滤功能。

图6-31 启用（取消）自适应过滤



6.4 网络特性

6.4.1 NAT配置

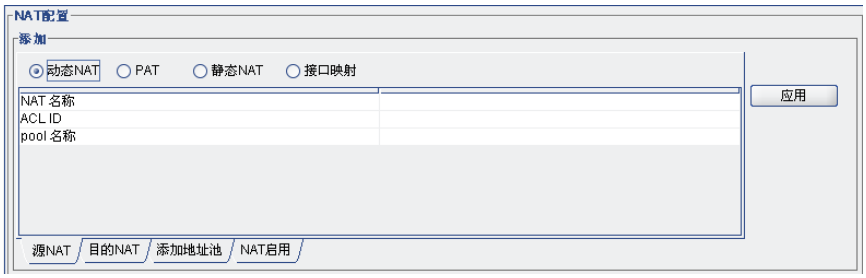
1．添加 NAT

1）源 NAT

■ 动态 NAT

如图 6-32 所示，该种类型的 NAT 需要用户输入 NAT 名称、选择 ACL ID 和 pool 名称，然后按添加键即可添加成功。

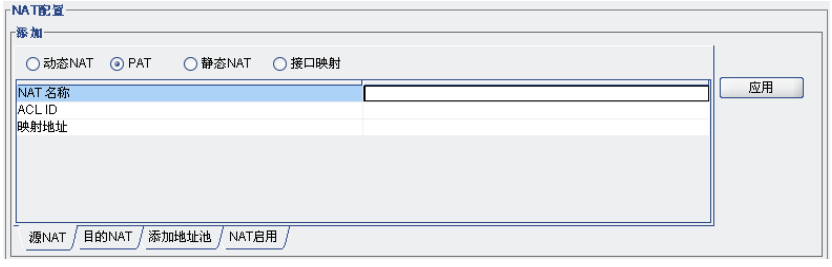
图6-32 添加动态 NAT



■ PAT

如图 6-33 所示，该种类型的 NAT 需要用户输入 NAT 名称和映射地址、选择 ACL ID，然后按添加键即可添加成功。

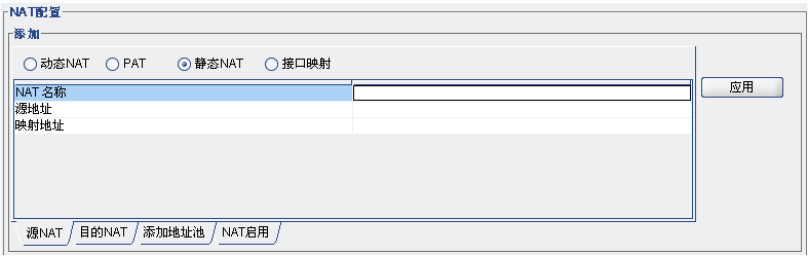
图6-33 添加 PAT



■ 静态 NAT

如图 6-34 所示，该种类型的 NAT 需要用户输入 NAT 名称、源地址、映射地址，然后按添加键即可添加成功。

图6-34 添加静态 NAT



■ 接口映射

如图 6-35 所示，该种类型的 NAT 需要用户输入 NAT 名称、选择 ACL ID 和接口名称，然后按添加键即可添加成功。

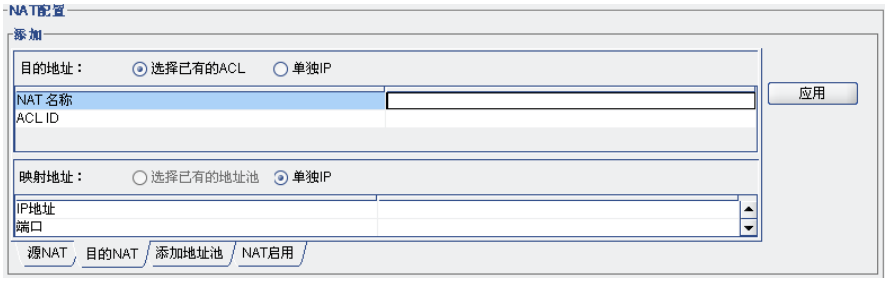
图6-35 添加接口映射

2）目的 NAT

■ 目的地址：选择已有的 ACL，映射地址：单独 IP

如图 6-36 ，在目的地址一栏，用户需要输入 NAT 名称，选择 ACL ID；在映射地址一栏，用户需要输入 IP 地址和端口；都输入完成后，按添加键即可添加成功。

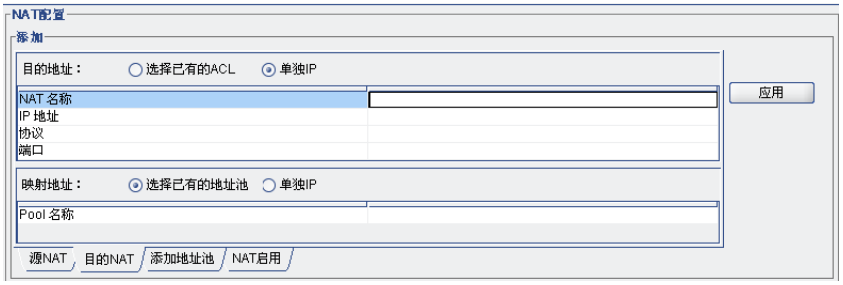
图6-36 添加目的 NAT



■ 目的地址：单独 IP；映射地址：选择已有的地址池

如图 6-37 ，在目的地址一栏，用户需要输入 NAT 名称、IP 地址、端口、选择协议；在映射地址一栏，用户需要选择 Pool 名称；之后按添加键即可添加成功。

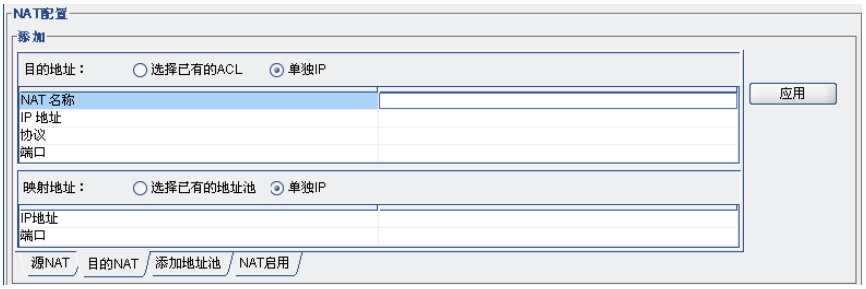
图6-37 添加目的 IP



■ 目的地址：单独 IP；映射地址：单独 IP

如图 6-38 ，在目的地址一栏，用户需要输入 NAT 名称、IP 地址、端口、选择协议；在映射地址一栏，用户需要输入 IP 地址、端口；之后用户按添加键即可添加成功。

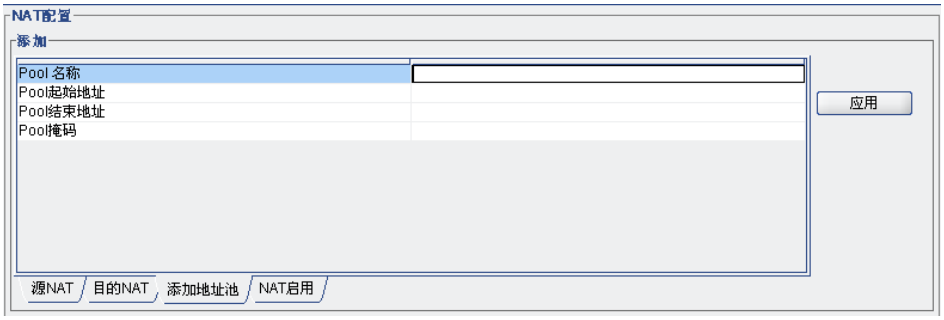
图6-38 添加目的 IP



3）添加地址池

如图 6-39 所示，用户需要输入 Pool 名称、Pool 起始的 IP 地址、Pool 结束的 IP 地址，选择 Pool 掩码的位数，选定好之后，按添加键即可添加成功。

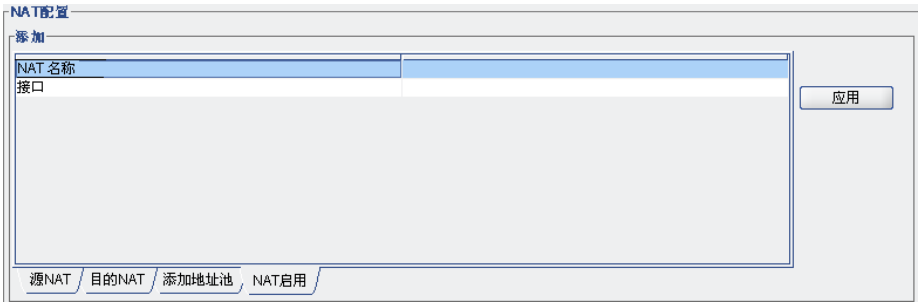
图6-39 添加地址池



4）NAT 启用

如图 6-40 所示，用户需要选择 NAT 名称和接口名字，选好之后按应用键在该接口启用该 NAT。

图6-40 NAT 启用



2．删除 NAT

1）删除 NAT

如图 6-41 所示，用户需要在 NAT 名称一栏选择某个 NAT，选定好之后，按删除键进行删除。

图6-41 删除 NAT

2）删除地址池

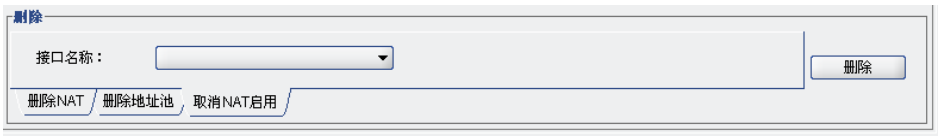
如图 6-42 所示，用户需要在 Pool 名称一栏选择某个 Pool，选定好之后，按删除键进行删除。

图6-42 删除地址池

3）取消 NAT 启用

如图 6-43 所示，用户需要在接口名称一栏选择某个接口。

图6-43 取消 NAT 启用

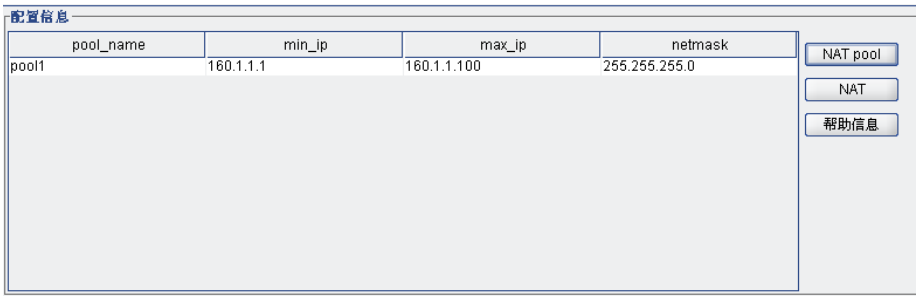


3．查看配置信息

1）查看 NAT Pool 信息

如图 6-44 ，用户通过点击“NAT Pool”键，可以查看到 NAT Pool 信息。

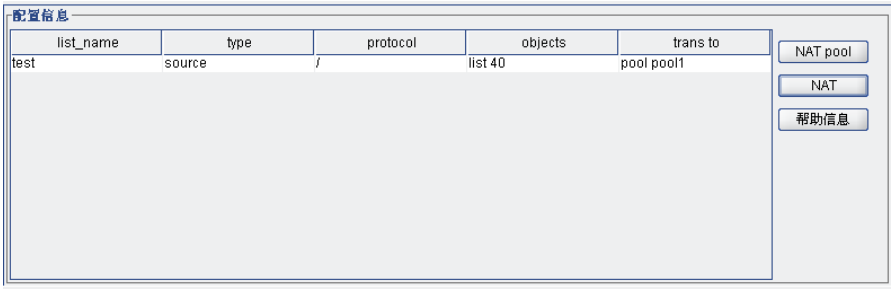
图6-44 NAT Pool 信息



2）查看 NAT 信息

如图 6-45 ，用户通过点击 NAT 键，可以查看 NAT 信息。

图6-45 NAT 信息



6.5 路由功能

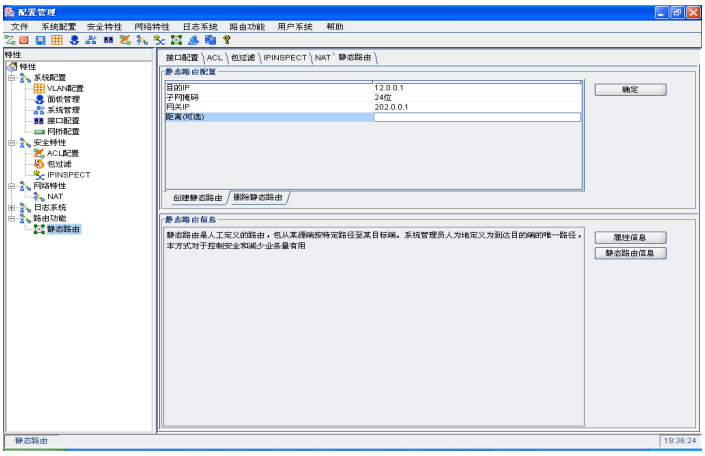
6.5.1 静态路由

静态路由是人工定义的路由，包从某源端按特定路径至某目标端。系统管理员人为地定义为到达目的端的唯一路径，本方式对于控制安全和减少业务量有用。

1） 创建静态路由

如图 6-46 所示，用户可以输入目的 IP 地址，子网掩码位数，网关 IP，距离（可选），按确定键即可将创建好的静态路由加入到路由表中。

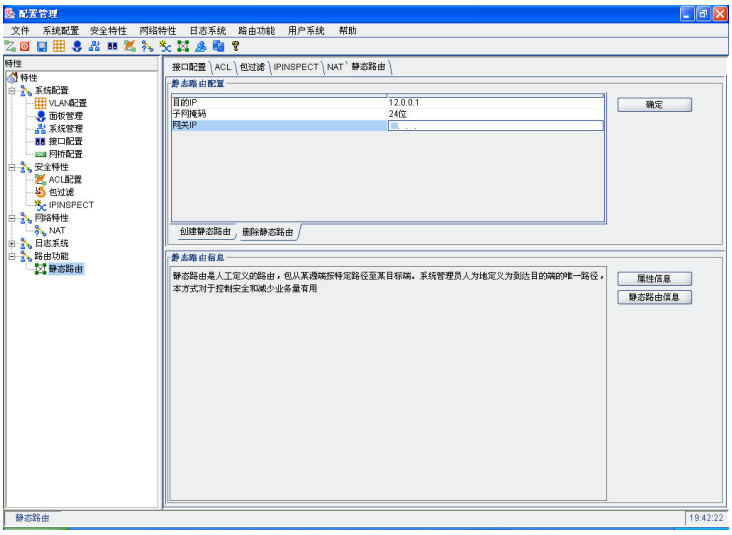
图6-46 创建静态路由



2） 删除静态路由

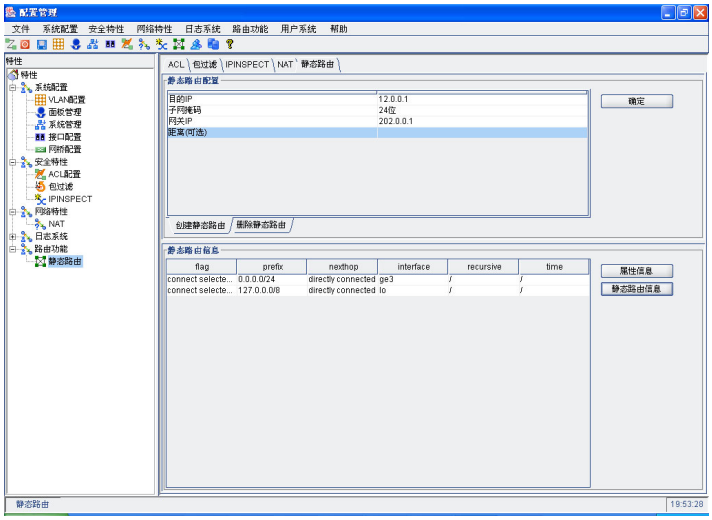
如图 6-47 所示，用户输入要删除的静态路由的 IP 地址，子网掩码位数，网关 IP，按确定键后即可从路由表中删除该条静态路由。

图6-47 删除静态路由



用户还可以通过点击静态路由信息按钮来查看当前的静态路由信息，如图 6-48 所示。

图6-48 静态路由信息



注意

命令执行过程中，需要的时间根据网络状况，可能会有很大的差异。网络拥塞，速度有可能较慢，请耐心等候。

7 日志管理

7.1 概述

日志管理主要是对系统中的各个事件作日志记录。当系统发生某一个故障的时候，可以借助日志管理系统来定位哪个设备和哪个操作人员进行的操作，对故障的定位和排除提供依据。还可以查看 NetFlow 流量，生成各种报表。

日志管理主要包括 Syslog 日志和 NetFlow 日志管理功能，其中：

- Syslog 日志主要是提供对操作人员操作的查询，比如新建用户、新建操作员等管理信息；
- NetFlow 日志主要是对 VPN 业务的支持，如添加新的 VPN 业务，增加、修改 VRF 和 CERC 信息等业务相关的数据；

7.2 Syslog日志管理

Syslog 日志管理主要是提供管理员对 Syslog 日志的查看功能，同时还提供打印和保存功能。前台界面如下所示，Syslog 日志前台提供给用户的信息包括日志 ID，日志接收时间，主机名，Syslog 类型，级别信息，日志详情。用户点击每一列的列头，日志信息会以该列的信息重新排列。用户可以直接定位到最后一页显示最后日志信息，也可以按“上一页”、“下一页”按钮查看上下信息。用户还可以根据自己的需要选择显示第一页显示的行数，日志管理提供给用户四种选择：100、200、500、1000。

用户还可以对日志信息进行删除，删除条件包括时间范围、日志类型。日志删除界面如图 7-1 所示。

要对 Syslog 日志系统进行查询，请选择工具菜单项下的“查询”，弹出日志过滤窗口，如图 7-1 所示，查询条件包括：

时间：

- 开始/结束时间：可以通过选择起始和结束时间，查询满足该时间段的日志信息；

- 相对时间段：可以通过选择相对时间段，查询满足该时间段的日志信息。相对时间段包括：24 小时、48 小时、36 小时、当月、所有。分别代表相对于查询操作时间前 24 小时、前 48 小时、前 36 小时、当月和全部的日志信息。查询结果为满足该查询条件的所有日志信息；

主机名

按照主机名，查询特定主机的 Syslog 日志；

日志类型

按照日志类型，查询特定日志类型的 Syslog 日志。下拉框中的日志类型是当前表中包含的所有日志类型；

详情匹配

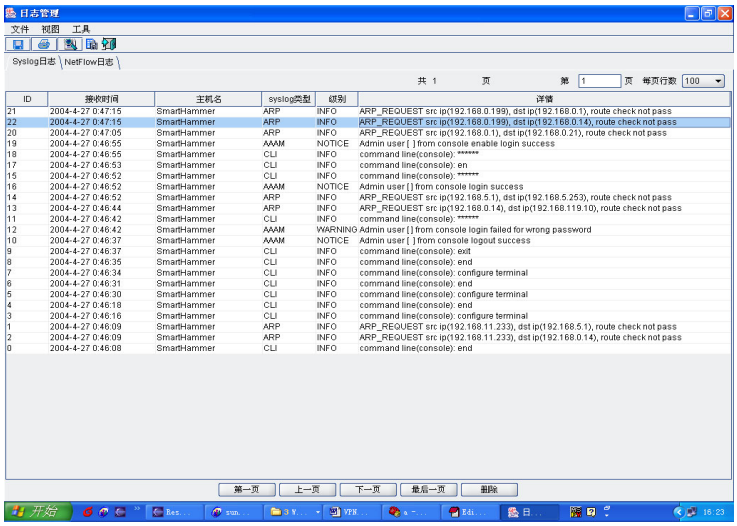
对输入详情中的任意字段进行匹配，查询结果为详情信息中包含输入字段的所有日志信息；

日志级别

按照 Syslog 日志的级别进行查询。Syslog 日志共有七种级别信息，分别为 EMERG、ALERT、CRITICAL、ERROR、WARNING、NOTICE、 INFORMATION；对应的数字级别信息分别为： 0、1、2、3、4、5、6。如果选择“空”，系统显示所有日志级别的日志信息。下拉框中的日志级别是当前表中包含的所有日志级别；

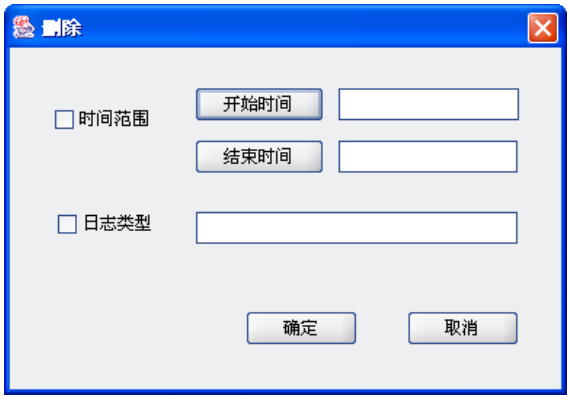
Syslog 日志管理的前台界面如图 7-1 所示：

图7-1 Syslog 日志管理的前台界面



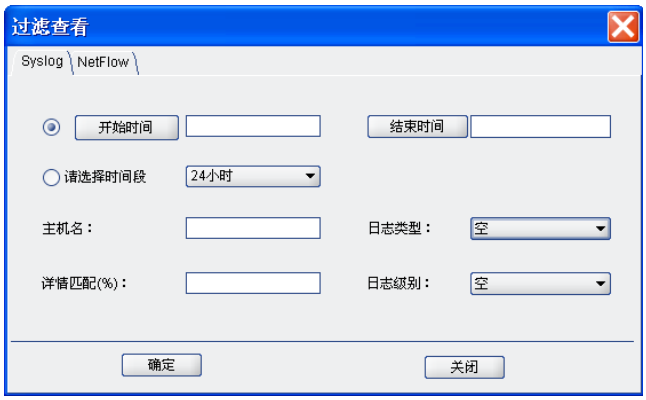
删除日志界面如图 7-2 所示：

图7-2 删除日志界面



Syslog 查询界面如图 7-3 所示：

图7-3 查询界面



如果某一项没有选择或填写，则表示查询此项的所有内容；在过滤查看中必须提供查询时间。

对于 Syslog，用户可以根据日志级别、日志类型、主机名来生成报表，方法是用户选定上述类型的某一项，选择好开始时间和结束时间，按“确定”按钮即可生成所需要的报表。如要显示统计数据前 10 位的报表，选取“显示 TOP10”复选框，按“确定”按钮。报表包括饼状图、柱状图和数据表格供用户查看。

选取查看项目:

包括按日志级别统计条数（百分比=条数/总条数）、按日志类型统计条数（百分比=条数/总条数）、按主机名统计条数（百分比=条数/总条数）；

时间：

- 开始时间/结束时间：可以通过选择起始和结束时间，查询满足该时间段的日志信息；
- 相对时间段：可以通过选择相对时间段，查询满足该时间段的日志信息。相对时间段包括：24 小时、48 小时、36 小时、当月、所有。分别代表相对于查询操作时间前 24 小时、前 48 小时、前 36 小时、当月和全部日志信息。查询结果为满足该查询条件的所有日志信息；

TOP10:

是否只显示前 10 位统计数据；

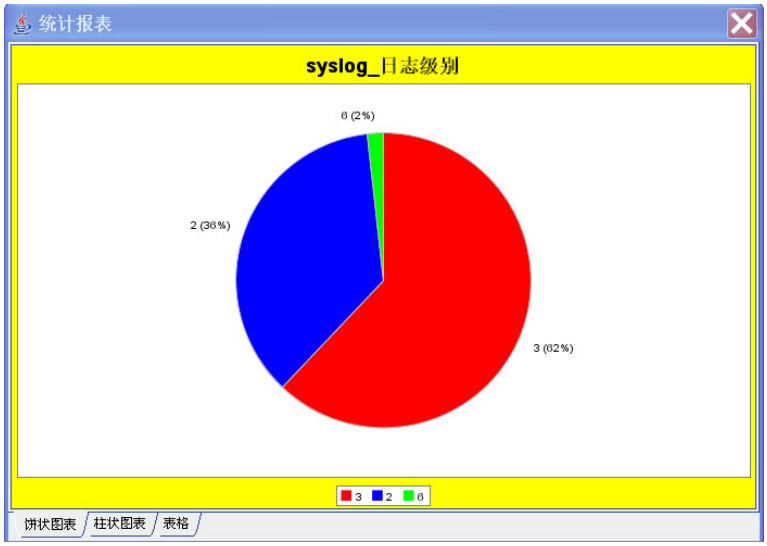
Syslog 报表查询界面如图 7-4 所示：

图7-4 Syslog 报表查询

如果某一项没有选择或填写，则表示查询此项的所有内容；在过滤查看中必须提供查询时间。

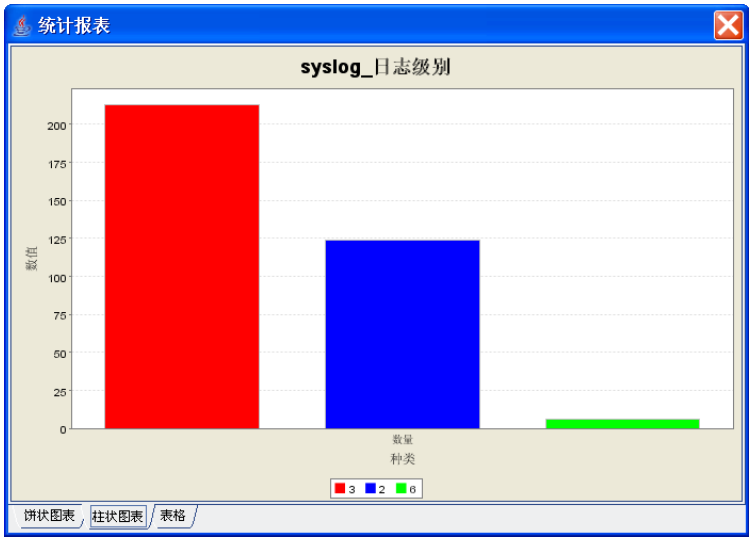
Syslog 报表饼状图显示如图 7-5 所示：

图7-5 Syslog 报表饼状图



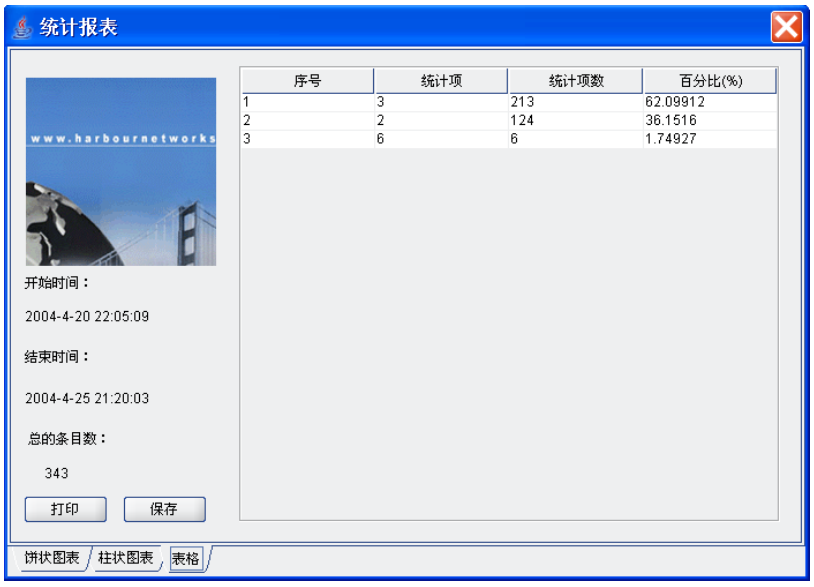
Syslog 报表柱状图显示如图 7-6 所示：

图7-6 Syslog 报表柱状图



Syslog 报表表格显示如下图所示：

图7-7 Syslog 报表表格图形



- “打印”按钮：提供打印统计结果表格中数据的功能；
- “保存”按钮：提供保存统计结果表格中数据的功能，保存文件格式*.xls；

7.3 NetFlow日志管理

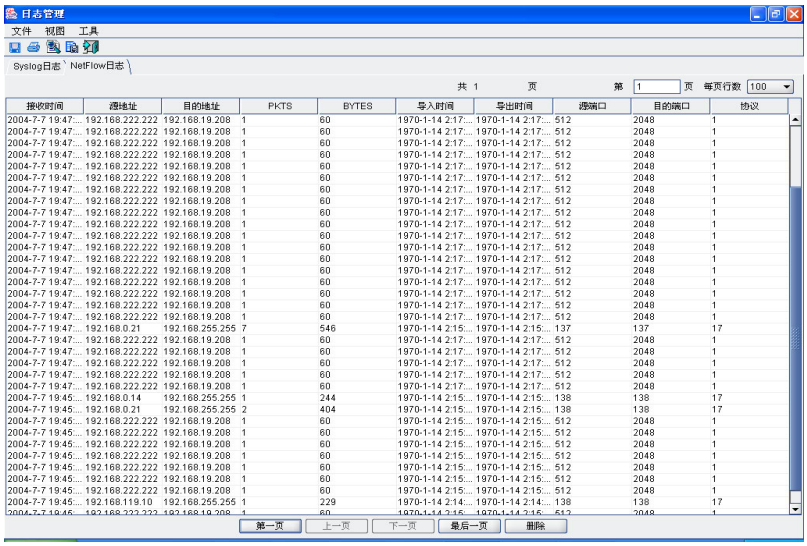
NetFlow 日志是记录网络流量的关键日志。NetFlow 日志管理主要是提供对 NetFlow 日志的查看和查询，并提供报表的打印和保存功能。

NetFlow 日志的前台界面图 7-8 所示，NetFlow 日志前台界面提供给用户的信息包括接收时间、源地址、目的地址、包数、字节数、导入时间、导出时间、源端口、目的端口、协议。用户点击每一列的列头，日志信息会以该列的信息重新排列。用户可以直接定位到最后一页显示日志的最后信息，也可以按上一页、下一页查看相关信息。用户还可以根据自己的需要选择显示的行数。

日志管理提供给用户四种选择：100、200、500、1000。用户还可以对日志信息进行删除操作，删除条件包括时间范围、日志类型。界面如下图所示。

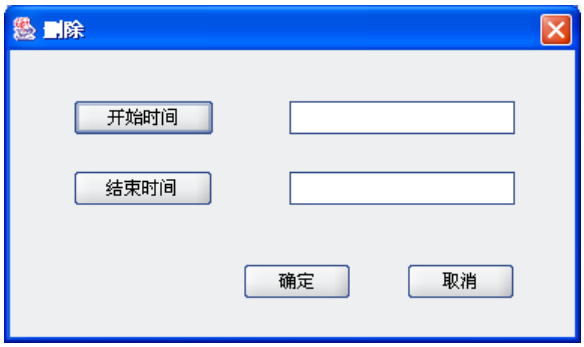
NetFlow 日志管理的前台界面如图 7-8 所示：

图7-8 NetFlow 日志管理前台界面



NetFlow 删除操作前台界面如图 7-9 所示：

图7-9 NetFlow 日志删除操作前台界面



查询条件包括：

时间：

开始/结束时间：可以通过选择起始和结束时间，查询满足该时间段的日志信息；

相对时间段：可以通过选择相对时间段，查询满足该时间段的日志信息。相对时间段包括：24 小时、48 小时、36 小时、当月、所有。分别代表相对于查询操作时间前 24 小时、前 48 小时、前 36 小时、当月和全部日志信息。查询结果为满足该查询条件的所有日志信息；

根据协议类型进行查询：

按照协议类型名称，查询特定日志类型的 NetFlow 日志。下拉框中的协议类型是当前表中包含的所有类型；

源地址：

- 完整的 IP 字符串：当输入字符串为完整的 IP 字符串时（如：192.168.1.23），查询结果为源地址为该 IP 的所有日志信息；
- 不完整 IP 字符串：当输入字符串为不完整的 IP 字符串时（如：192.168.*.*），查询结果为源地址在该 IP 字符串网段（这时网段为 192.268.0.0~192.168.255.255）内的所有日志信息；

源端口：根据输入的源端口进行查:

目的地址：

- 完整的 IP 字符串：当输入字符串为完整的 IP 字符串时（如：192.168.1.23），查询结果为目的地址为该 IP 的所有日志信息；
- 不完整 IP 字符串：当输入字符串为不完整的 IP 字符串时（如：192.168.*.*），查询结果为目的地址在该 IP 字符串网段（这时网段为 192.268.0.0~192.168.255.255）内的所有日志信息；

目的端口：

根据输入的目的端口进行查询；

图7-10 NetFlow 日志查询

注意

如果某一项没有选择或填写，则表示查询此项的所有内容；在过滤查看中必须提供查询时间。

对于 NetFlow，用户可以根据源地址、目的地址、源端口、目的端口、目的端口流量、源地址流量、目的地址流量、源地址到目的地址统计来生成报表，方法是用户选定上述类型的某一项，选择好开始时间和结束时间，按确定键即可生成所需要的报表。如要显示统计数据前 10 位的报表，选取“显示 TOP10”复选框，按“确定”按钮。NetFlow 报表提供饼状图、柱状图、曲线图供用户查看。

选取查看项目：

包括按源地址统计日志条数（百分比=条数/总条数）、按目的地址统计日志条数（百分比=条数/总条数）、按源端口统计日志条数（百分比=条数/总条数）、按目的端口统计日志条数（百分比=条数/总条数）、按目的端口统计流量（百分比=流量/总流量）、按源地址统计流量（百分比=流量/总流量）、按目的地址统计流量（百分比=流量/总流量）、按源地址到目的地址统计日志条数（百分比=条数/时间）；

时间：

- 开始时间/结束时间：可以通过选择起始和结束时间，查询满足该时间段的日志信息；
- 相对时间段：可以通过选择相对时间段，查询满足该时间段的日志信息。相对

时间段包括：24 小时、48 小时、36 小时、当月、所有。分别代表相对于查询操作时间前 24 小时、前 48 小时、前 36 小时、当月和全部日志信息。查询结果为满足该查询条件的所有日志信息；

TOP10：

是否只显示前 10 位统计数据；

NetFlow 报表查询界面如图 7-11 所示：

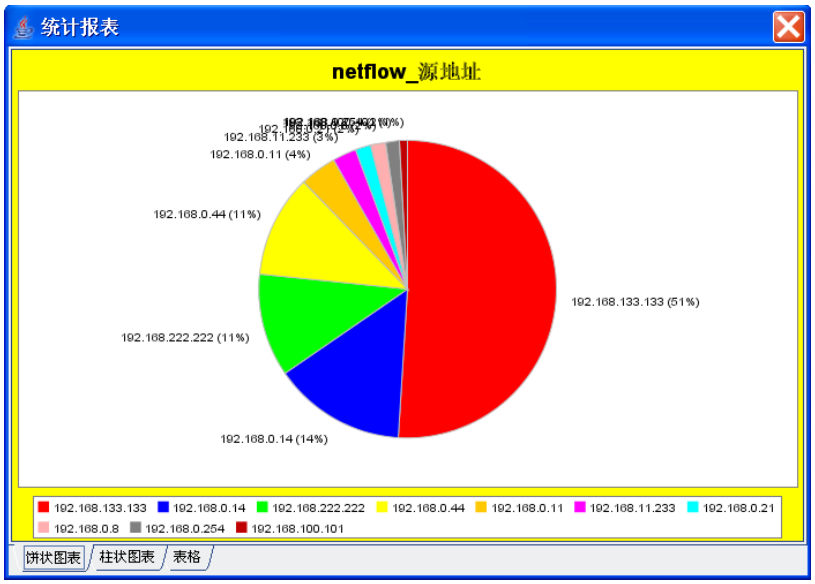
图7-11 日志报表

注意

如果某一项没有选择或填写，则表示查询此项的所有内容；在过滤查看中必须提供查询时间。

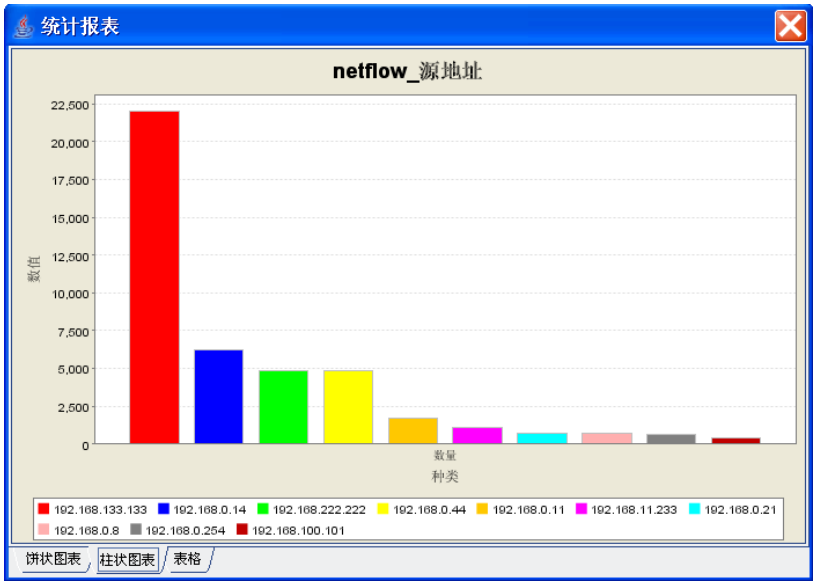
NetFlow 报表饼状图显示如图 7-12 所示：

图7-12 NetFlow 报表饼状图



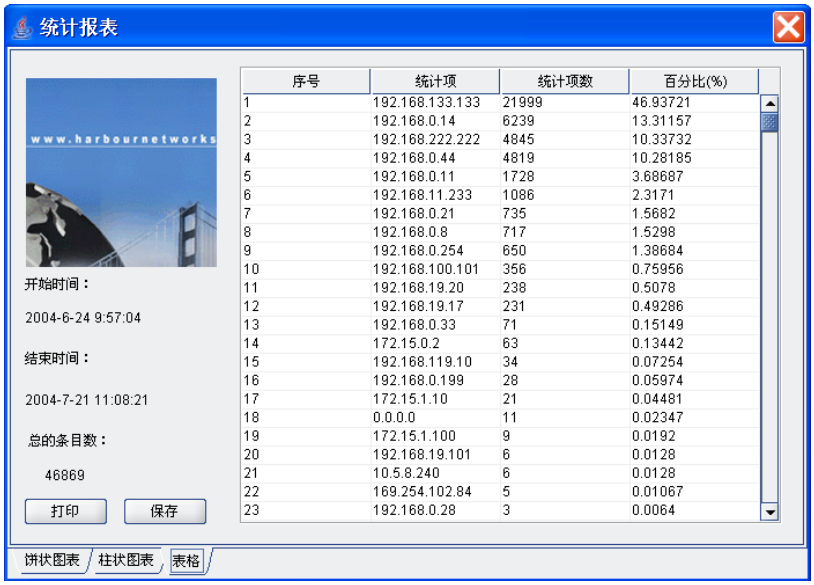
NetFlow 报表柱状图显示如图 7-13 所示：

图7-13 NetFlow 报表柱状图



NetFlow 报表表格显示如图 7-14 所示：

图7-14 NetFlow 报表表格



序号	统计项	统计项数	百分比(%)
1	192.168.133.133	21999	46.93721
2	192.168.0.14	6239	13.31157
3	192.168.222.222	4845	10.33732
4	192.168.0.44	4819	10.28185
5	192.168.0.11	1728	3.68687
6	192.168.11.233	1086	2.3171
7	192.168.0.21	735	1.5682
8	192.168.0.8	717	1.5298
9	192.168.0.254	650	1.38684
10	192.168.100.101	356	0.75956
11	192.168.19.20	238	0.5078
12	192.168.19.17	231	0.49286
13	192.168.0.33	71	0.15149
14	172.15.0.2	63	0.13442
15	192.168.119.10	34	0.07254
16	192.168.0.199	28	0.05974
17	172.15.1.10	21	0.04481
18	0.0.0.0	11	0.02347
19	172.15.1.100	9	0.0192
20	192.168.19.101	6	0.0128
21	10.5.8.240	6	0.0128
22	169.254.102.84	5	0.01067
23	192.168.0.28	3	0.0064

- “打印”按钮：提供打印统计结果表格中数据的功能；
- “保存”按钮：提供保存统计结果表格中数据的功能，保存文件格式*.xls；